

SÉRIE A, N° 2644

N° D'ORDRE :

3516

THÈSES

PRÉSENTÉES

A LA FACULTÉ DES SCIENCES
DE L'UNIVERSITÉ DE PARIS

POUR OBTENIR

LE GRADE DE DOCTEUR ÈS SCIENCES MATHÉMATIQUES

PAR BERNARD CHARLES

1^{re} THÈSE. — SUR L'ALGÈBRE DES OPÉRATEURS LINÉAIRES.

2^e THÈSE. — PROPOSITIONS DONNÉES PAR LA FACULTÉ.

Soutenues le 16 juin 1953 devant la Commission d'examen.

MM. JULIA,

DUBREIL,

SCHWARTZ,

Président.

Examineurs.

PARIS

GAUTHIER-VILLARS, ÉDITEUR-IMPRIMEUR-LIBRAIRE

Quai des Grands-Augustins, 55

1954

SÉRIE A, N° 2644

N° D'ORDRE :

3516

THÈSES

PRÉSENTÉES

A LA FACULTÉ DES SCIENCES
DE L'UNIVERSITÉ DE PARIS

POUR OBTENIR

LE GRADE DE DOCTEUR ÈS SCIENCES MATHÉMATIQUES

PAR BERNARD CHARLES

1^{re} THÈSE. — SUR L'ALGÈBRE DES OPÉRATEURS LINÉAIRES.

2^e THÈSE. — PROPOSITIONS DONNÉES PAR LA FACULTÉ.

Soutenues le 16 juin 1953 devant la Commission d'examen.

MM. JULIA,

Président.

DUBREIL,

SCHWARTZ,

} *Examineurs.*

PARIS

GAUTHIER-VILLARS, ÉDITEUR-IMPRIMEUR-LIBRAIRE

Quai des Grands-Augustins, 55

—
1954

FACULTÉ DES SCIENCES DE L'UNIVERSITÉ DE PARIS

Doyen..... M. A. CHATELET.

PROFESSEURS

G. JULIA.....	T	Analyse supérieure et Algèbre supérieure.	CHRÉTIEN.....	T	Chimie minérale.
A. DENJOY.....	T	Théorie des fonctions.	P. DRACH.....	T	Zoologie.
L. LUTAUD.....	T	Géographie physique et Géologie dynamique.	KASTLER.....	T	Physique.
E. DARMOIS.....	T	Enseignement de Physique.	CHATELET.....	T	Arithmétique et théorie des nombres.
ROBERT LÉVY.....	T	Physiologie comparée.	EPHRUSSI.....	T	Génétique.
FOCH.....	T	Mécanique physique et expérimentale.	WURMSER.....	T	Biologie physico-chimique.
PAUTHENIER.....	T	Électrotechnique générale.	BAUER.....	T	Chimie-Physique.
DE BROGLIE.....	T	Théories physiques.	RIVIÈRE.....	T	Géologie (P. C. B.).
JOB.....	T	Chimie générale.	GAUTHERET.....	T	Biologie végétale (P. C. B.).
PRENANT.....	T	Anatomie et Histologie comparées.	LUCAS.....	T	Physique.
COMBES.....	T	Physiologie végétale.	A. THOMAS.....	T	Évolution des êtres organisés.
GARNIER.....	T	Géométrie supérieure.	ARNULF.....	T	Optique appliquée.
PERÈS.....	T	Mécanique des fluides et applications.	MAX MORAND.....	T	Physique.
LAUGIER.....	T	Physiologie générale.	SOLEILLET.....	T	Physique.
TOUSSAINT.....	T	Technique aéronautique.	FORTIER.....	T	Mécanique expérimentale des fluides.
M. CURIE.....	T	Physique (P. C. B.).	DANJON.....	T	Astronomie.
G. RIBAUD.....	T	Hautes températures.	FROMAGEOT.....	T	Chimie biologique.
CHAZY.....	T	Mécanique analytique et Mécanique céleste.	LAPORTE.....	T	Physique générale et Radio-activité.
CROZE.....	T	Physique théorique et Physique céleste.	JANET.....	T	Mathématiques générales.
DUPONT.....	T	Théories chimiques.	PETIT.....	T	Biologie maritime.
VALIRON.....	T	Calcul différentiel et Calcul intégral.	QUENEY.....	T	Météorologie et dynamique atmosphérique.
BARRABÉ.....	T	Géologie structurale et Géologie appliquée.	GALLIEN.....	T	Biologie animale (P. C. B.).
G. DARMOIS.....	T	Calcul des probabilités et Physique mathématique.	EICHHORN.....	T	Biologie végétale (P. C. B.).
JACQUES BOURCART	T	Géographie physique et Géologie dynamique.	DE CUGNAC.....	T	Biologie végétale (P. C. B.).
AUBEL.....	T	Chimie biologique.	M ^{lle} CAUCHOIS.....	T	Chimie-Physique.
M ^{me} JOLIOT-CURIE.	T	Physique générale et Radio-activité.	THELLIER.....	T	Physique du Globe.
PLANTEFOL.....	T	Botanique.	AUDUBERT.....	T	Électrochimie.
CABANNES.....	T	Recherches physiques.	L'HÉRITIER.....	T	Génétique.
GRASSÉ.....	T	Évolution des êtres organisés.	GRIVET.....	T	Radioélectricité.
PRÉVOST.....	T	Chimie organique.	PONCIN.....	T	Mécanique des fluides.
BOULIGAND.....	T	Application de l'analyse à la Géométrie.	THIRY.....	T	Mécanique appliquée.
CHAUDRON.....	T	Chimie appliquée.	DUBREIL.....	T	Mathématiques générales.
WYART.....	T	Minéralogie.	QUELET.....	T	Chimie (P. C. B.).
TEISSIER.....	T	Zoologie.	CAGNIARD.....	T	Géophysique appliquée.
MANGENOT.....	T	Biologie végétale.	CHAMPETIER.....	T	Chimie appliquée.
P. AUGER.....	T	Physique quantique et relativité.	CUVILLIER.....	T	Géologie structurale et Géologie appliquée.
MONNIER.....	T	Physiologie générale.	JUNG.....	T	Pétrographie.
PIVETEAU.....	T	Géologie.	TRILLAT.....	T	Physique (P. C. B.).
ROCARD.....	T	Physique.	WIEMANN.....	T	Chimie (P. C. B.).
H. CARTAN.....	T	Mathématiques (E. N. Supérieure).	JACQUINOT.....	T	Physique (P. C. B.).
SCHAEFFER.....	T	Physiologie des fonctions.	VASSY.....	T	Physique de l'atmosphère.
LAFFITE.....	T	Chimie générale.	DESTOUCHES.....	T	Théories physiques.
FAVARD.....	T	Mécanique générale.	M. PRUVOST.....	T	Géologie.
COULOMB.....	T	Physique du Globe.	AMIEL.....	T	Chimie (P. C. B.).
M ^{lle} COUSIN.....	T	Biologie animale (P. C. B.).	HOCART.....	T	Minéralogie.
			MACHEBOEUF.....	T	Microbiologie.
			J.-P. MATHIEU.....	T	Physique (P. C. B.).
			COUTEAUX.....	T	Biologie animale (P. C. B.).
			MAY.....	T	Biologie animale (P. C. B.).
			CHOQUET.....	T	Calcul différentiel.
			FELDMANN.....	T	Biologie (P. C. B.).
			GUINIER.....	T	Physique (P. C. B.).
			JOST.....	T	Biologie (P. C. B.).

Secrétaire..... CH. MONIER.



A MA MÈRE



Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41552217_0030

PREMIÈRE THÈSE.

Sur l'algèbre des opérateurs linéaires.

INTRODUCTION.

Dans ce travail on étudie l'algèbre des opérateurs linéaires en s'attachant plus spécialement aux propriétés de commutativité.

Dans le chapitre I on passe en revue les propriétés d'un opérateur linéaire A sur un espace vectoriel à n dimensions (hypothèse conservée dans les deux chapitres suivants). On étudie les sous-espaces stables pour A .

Dans le chapitre II on commence par étudier l'anneau $r'(A)$ des commutants de A et son centre $r''(A)$. On donne une démonstration très simple du théorème classique $r''(A) = r(I, A)$ sous une forme un peu plus générale. La fin du chapitre est consacrée à l'étude de la permutabilité. Le théorème 19 donne deux conditions nécessaires pour que deux opérateurs linéaires permutables soient fonctions d'un même troisième. Cette question avait été posée par G. Frobenius [6]; le premier contre-exemple a été donné par H. B. Phillips [16], mais la réponse négative à la question de G. Frobenius était déjà virtuellement contenue dans un Mémoire de C. Jordan [9].

Le chapitre III est consacré à l'étude des anneaux commutatifs d'opérateurs linéaires. On démontre que si le corps de base est parfait on peut se ramener à l'étude d'anneaux nilpotents. Diverses propriétés sont démontrées. On s'occupe surtout des anneaux commutatifs maximaux, c'est-à-dire non contenus dans un anneau commutatif plus grand. On détermine un certain nombre d'anneaux particuliers, ce

qui est l'occasion de rectifier une erreur d'un Mémoire de C. Jordan[9]. A la fin du chapitre on précise les relations entre l'étude des anneaux commutatifs et celle des systèmes hypercomplexes. On en tire quelques applications : Énoncé d'un critère de maximalité qui, en particulier, permet toujours de conclure lorsque l'espace a moins de six dimensions; formation d'un exemple général d'anneau commutatif tel que $R'' \neq r(R, I)$.

Dans le chapitre IV on passe à l'étude d'un opérateur linéaire sur un espace vectoriel quelconque. On utilise presque exclusivement le langage des groupes abéliens à opérateurs. Deux cas sont surtout envisagés, qui correspondent à un groupe primaire ou à un groupe de rang 1. Dans le premier cas on montre que $r''(A)$ coïncide avec la fermeture de $r(I, A)$ pour la topologie finie, résultat qui à notre connaissance n'avait pas encore été publié⁽¹⁾. Dans le deuxième cas on montre que la plupart des propriétés des opérateurs linéaires non dérogoires se généralisent.

Dans le chapitre V on s'occupe des anneaux commutatifs dont les projecteurs forment un treillis complet. Les propriétés démontrées présentent une certaine analogie avec celles de l'anneau engendré par un opérateur autoadjoint dans un espace de Hilbert. Par exemple R'' coïncide avec la fermeture de $r(R, I)$ pour la topologie finie, on peut aussi décomposer le spectre de R en une partie ponctuelle et une partie continue. Mais tout ce qu'on fait ici a un caractère purement algébrique.

Les principaux résultats de ce travail ont été résumés dans quelques Notes aux *Comptes rendus de l'Académie des Sciences* ⁽²⁾.

Je tiens à remercier M. J. Dixmier de ses conseils amicaux et de ses encouragements constants, M. le professeur N. Jacobson des indications précieuses qu'il m'a données, M. le professeur P. Dubreil de sa bienveillance et des suggestions qu'il a bien voulu me faire.

⁽¹⁾ M. I. Kaplansky nous signale qu'il a obtenu ce résultat, indépendamment et sous une forme un peu différente. Nous démontrons d'ailleurs un résultat un peu plus général au théorème 33.

⁽²⁾ *C. R. Acad. Sc.*, t. 236, 1953, p. 990, 1122-1123, 1722-1723, 1835-1837 et 2027-2029.

J'exprime toute ma reconnaissance à M. le professeur G. Julia qui m'a fait le grand honneur d'accepter la présidence de cette thèse. Je tiens aussi à remercier M. le professeur L. Schwartz d'avoir bien voulu s'intéresser à ce travail.

Nous pensons utile de préciser maintenant quelques notations et résultats qui seront utilisés dans la suite.

Un groupe abélien à opérateur est un groupe abélien E , noté additivement, sur lequel opèrent les éléments d'un anneau R avec les conditions :

- (1) $a(u + v) = au + av \quad (a \in R; u, v \in E);$
- (2) $(a + b)u = au + bu \quad (a, b \in R; u \in E);$
- (3) $(ab)u = a(bu) \quad (a, b \in R; u \in E);$
- (4) R contient un élément unité qui est opérateur identique.

Nous dirons brièvement que E est un groupe abélien sur R . Si plusieurs anneaux opèrent sur le même groupe E , nous utiliserons la notation E_R pour désigner E considéré comme groupe abélien sur R . Enfin si E n'a pas d'anneau d'opérateurs, on considérera l'anneau des nombres entiers comme anneau d'opérateurs.

Un sous-groupe de E est une partie F de E qui possède les propriétés :

- (5) $u, v \in F \quad \text{entraîne} \quad u - v \in F;$
- (6) $u \in F, \quad a \in R \quad \text{entraîne} \quad au \in F.$

Soit E et F deux groupes abéliens sur le même anneau R . T étant un homomorphisme de E dans F posons

$$\bar{T}^{-1}(0) = \{ u \in E \mid Tu = 0 \} = \text{ensemble des } u \in E \text{ tels que } Tu = 0.$$

$\bar{T}^{-1}(0)$ est un sous-groupe de E . Soit $\bar{u}$ la classe de u modulo $\bar{T}^{-1}(0)$, en posant $\bar{u} + \bar{v} = \overline{u + v}$, $a\bar{u} = \overline{au}$, on obtient un groupe sur R que l'on note $E/\bar{T}^{-1}(0)$, ou si il n'y a pas de confusion à craindre $\bar{E}$. La transformation $\bar{T} : \bar{u} \rightarrow Tu$ est un isomorphisme de $E/\bar{T}^{-1}(0)$ dans F .

$F_1, \dots, F_s$ étant des parties de E on note $(F_1, \dots, F_s)$ le plus petit sous-groupe de E qui contient $F_1, \dots, F_s$. Si l'on a $E = (\{u_i \mid i \in I\})$ où les u_i sont des éléments de E , on dira que les u_i forment un système

de générateurs de E ; si $E = (u)$, où $u \in E$ on dira que E est monogène ou cyclique.

Soit F une partie de E , S une partie de R , on pose

$$SF = \{ au \mid a \in S, u \in F \}.$$

Si E est monogène on peut écrire $E = (u) = Ru$.

$N(F) = \{ a \in R \mid aF = 0 \}$ est un idéal gauche de R appelé annulateur de F . $F \subset G$ entraîne $N(F) \supset N(G)$.

$N(E)$ est un idéal bilatère de R , soit $\bar{a}$ la classe de $a \in R$ modulo $N(E)$ et $\bar{R}$ l'anneau de ces classes, obtenu en posant $\bar{a} + \bar{b} = \overline{a + b}$, $\bar{a}\bar{b} = \overline{ab}$. On peut considérer E comme groupe abélien sur $\bar{R}$ en posant $\bar{a}u = au$. On voit que les notions de sous-groupe dans E_R et $E_{\bar{R}}$ coïncident. On a d'autre part :

THÉORÈME 1. — *Si E est monogène il est isomorphe à $\bar{R} = R/N(E)$ considéré comme groupe abélien sur R .*

Démonstration. — $\bar{R}$ peut être considéré comme groupe abélien sur R en posant $\bar{b}\bar{a} = \overline{ba}$. Si $E = (u)$ on vérifie que la correspondance $T(a) = au$ est un homomorphisme de R sur E , on achève en remarquant que $T^{-1}(0) = N(E)$.

Si E est somme directe des sous-groupes E_i , $i \in I$, on écrit

$$E = \sum_{i \in I} E_i.$$

Supposons que $E = E' + E''$. La transformation T définie par $T(u' + u'') = u'$, $u' \in E'$, $u'' \in E''$ est un endomorphisme de E que nous appellerons projection sur E' parallèlement à E'' , ou simplement projection sur E' si il n'y a pas de confusion possible.

Rappelons maintenant quelques résultats d'algèbre.

THÉORÈME 2. — *Si $E = (u)$ et si R est commutatif, tout endomorphisme de E est de la forme $Tv = av$ où $a \in R$.*

Démonstration. — On a $Tu = au$, tout $v \in E$ est de la forme bu , d'où

$$Tv = Tbu = bTu = bau = abu = av.$$

Soit R un anneau d'intégrité (commutatif, à élément unité et sans diviseurs de zéro) tel que tout idéal de R soit principal (engendré par un seul élément). On note $(a_1, \dots, a_n)$ l'idéal engendré par $a_1, \dots, a_n \in R$. Tout idéal se décompose de façon unique en un produit d'idéaux premiers.

Si a et b sont premiers entre eux, c'est-à-dire si $(a, b) = (1)$ il existe $\lambda, \mu \in R$ tels que $\lambda a + \mu b = 1$. λ est unique modulo (b) et μ unique modulo (a) . Plus généralement on a :

THÉOREME 3. — *Si $a_1, \dots, a_s$ sont premiers entre eux deux à deux il existe $\lambda_1, \dots, \lambda_s \in R$ tels que $\sum_{i=1}^s \lambda_i \prod_{j \neq i} a_j = 1$; de plus λ_i est unique modulo (a_i) .*

THÉOREME 4. — *Si p est premier, $R/(p)$ est un corps.*

Pour toutes les questions d'algèbre nous renvoyons aux traités de P. Dubreil [4] et de B. L. van der Waerden [24].

CHAPITRE I.

OPÉRATEURS LINÉAIRES SUR UN ESPACE VECTORIEL A n DIMENSIONS.

I. — Espaces vectoriels. Opérateurs linéaires.

Soit E un groupe abélien sur un anneau R . Si R est un corps commutatif K on dit que E est un espace vectoriel sur K .

Un opérateur linéaire sur E est un endomorphisme de E .

L'ensemble des opérateurs linéaires A qui sont des applications biunivoques de E sur E est le groupe linéaire général de E ; on le note $GL(E, K)$; lorsque E a n dimensions, on utilise aussi la notation $GL(n, K)$; l'opérateur identique I est l'unité de ce groupe.

Deux opérateurs linéaires A et A' sont dits semblables si il existe $S \in GL(E, K)$ tel que $A' = S^{-1}AS$. La relation de similitude est une relation d'équivalence. La relation $A' = S^{-1}AS$ peut aussi être interprétée comme suit : Si A est représenté par la matrice A_Σ dans la base $\Sigma = \{u_1, \dots, u_n\}$, A sera représenté par la matrice $A_{s\Sigma} = S^{-1}A_\Sigma S$

dans la base $S\Sigma = \{Su_1, \dots, Su_n\}$. Notons que si $f(A)$ est un polynome en A , $A' = S^{-1}AS$ entraîne $f(A') = S^{-1}f(A)S$.

Dans toute la suite on étudie les propriétés des opérateurs linéaires qui se conservent par similitude, ou comme on dit aussi, qui sont invariantes relativement à $GL(E, K)$.

L'étude d'un opérateur linéaire A , à une similitude près, peut être ramenée à l'étude d'un groupe abélien à opérateurs, à une isomorphie près. Soit $R = K[x]$ l'anneau des polynomes en x à coefficients dans K . On peut construire un groupe abélien sur R en posant

$$f(x)u = f(A)u, \quad [f(x) \in R, u \in E].$$

On obtient bien ainsi un groupe abélien à opérateurs E_R .

Soit E'_R le groupe à opérateurs construit de façon analogue à partir de l'opérateur linéaire A' (E' désigne l'espace E lorsque A' opère sur lui).

Supposons que $A' = S^{-1}AS$ où $S \in GL(E, K)$. S^{-1} définit un isomorphisme de E_R sur E'_R car

$$\begin{aligned} S^{-1}(u + v) &= S^{-1}u + S^{-1}v \quad (u, v \in E); \\ S^{-1}(f(x)u) &= S^{-1}(f(A)u) = f(A')S^{-1}u = f(x)S^{-1}u \quad (f \in R, u \in E). \end{aligned}$$

Inversement si S^{-1} est un isomorphisme de E_R sur E'_R on peut écrire $A' = S^{-1}AS$ et $S \in GL(E, K)$.

L'étude de A à une similitude près se ramène donc à l'étude d'un groupe abélien à opérateurs à une isomorphie près. Ce point de vue très intéressant a été introduit par W. Krull [42], [43]; nous l'adopterons dans toute la suite.

II. — Étude d'un opérateur linéaire.

Soit A un opérateur linéaire et E_R le groupe à opérateurs construit à partir de A . On sait que :

- 1° $R = K[x]$ est commutatif contient un élément unité et est sans diviseurs de zéro;
- 2° Tout idéal de $R = K[x]$ est principal;
- 3° L'unité de $R = K[x]$ est opérateur identique.

Supposons maintenant que E a n dimensions. L'annulateur de E_R est un idéal (φ) de $R = K[x]$; nous allons montrer que $\varphi(x) \neq 0$. Entre les $n^2 + 1$ opérateurs linéaires $I, A, \dots, A^{n^2}$ il existe une relation

linéaire $f(A) = \sum_{i=0}^{n^2} \lambda_i A^i = 0$. Le polynôme $f(x)$ est $\neq 0$ et $\in (\varphi)$

donc $(\varphi) \neq 0$ ou si l'on préfère $\varphi(x) \neq 0$.

Finalement nous n'utiliserons pas en général l'hypothèse que E a n dimensions, mais la condition légèrement plus large;

4° L'annulateur de E est un idéal $(\varphi) \neq 0$.

Le polynôme φ qui engendre $N(E)$ n'est défini qu'à un facteur constant près. Nous fixerons ce facteur constant en convenant de prendre pour φ un polynôme dont le coefficient de la plus haute puissance de x vaut 1 (on dira que φ est normalisé). On peut définir φ comme le polynôme normalisé non nul de degré minimum parmi ceux qui vérifient $\varphi(A) = 0$. On appelle $\varphi(x)$ le polynôme minimal de A .

COMPOSANTES PRIMAIRES DE A . — THÉOREME 5. — Soit $\varphi = \varphi_1, \varphi_2, \dots, \varphi_s$ la décomposition de φ en facteurs primaires (φ_i , polynôme premier à la puissance α_i). E_R est somme directe des sous-groupes $E_i = \left(\prod_{j \neq i} \varphi_j \right) E$. De plus l'annulateur de E_i est (φ_i) .

Posons $\psi_i = \prod_{j \neq i} \varphi_j$. On vérifie que $E_i = \psi_i E$ est un sous-groupe de E_R .

Montrons que $E_R = \sum_{i=1}^s E_i$:

La somme est bien directe car si $u \in E_i \cap (\{E_j | j \neq i\})$, on a $\varphi_i u = 0$ et $\psi_i u = 0$, d'où $(\varphi_i, \psi_i)u = (1)u = 0$, d'où $u = 0$. Les E_i engendrent E ,

en effet : D'après le théorème 3 on peut écrire $1 = \sum_{i=1}^s f_i \psi_i$ avec $f_i \in R_i$.

On en déduit pour $u \in E$,

$$u = \sum_{i=1}^s f_i \psi_i u \quad \text{et} \quad \psi_i u \in \psi_i E = E_i.$$

Reste à montrer que $N(E_i) = (\varphi_i)$. On a $\varphi_i E_i = \varphi_i \psi_i E = \varphi E = 0$, donc $N(E_i) \supset (\varphi_i)$. D'autre part de $N(E_i) \psi_i E = 0$ on tire

$$N(E_i) \psi_i \subset (\varphi) = (\varphi_i)(\psi_i), \quad \text{d'où} \quad N(E_i) \subset (\varphi_i),$$

d'où finalement $N(E_i) = (\varphi_i)$.

Traduisons le théorème 5 pour A. On dit qu'un sous-espace F de E est stable pour A si $AF \subset F$. On voit que la notion de sous-espace stable pour A coïncide avec la notion de sous-groupe de E_R . E est

somme directe des sous-espaces stables E_i : $E = \sum_{i=1}^s E_i$. Dans E_i ,

A induit un opérateur A_i dont le polynôme minimal est φ_i . On dira que A_i est un opérateur primaire. A est somme directe des opéra-

teurs A_i , ce qu'on écrit $A = \sum_{i=1}^s A_i$. Les A_i sont les composantes primaires de A.

L'étude d'un opérateur quelconque se trouve ramenée à celle d'un opérateur primaire.

THÉOREME 6. — *Il existe un polynôme $g_i(A)$ qui induit zéro dans $E_j (j \neq i)$ et 1 dans E_i .*

Partons de $\psi_i(x)$ qui vérifie déjà $\psi_i u = 0$, $u \in E_j (j \neq i)$. Comme $(\varphi_i, \psi_i) = (1)$ il existe $f_i \in R$ tel que $f_i \psi_i \equiv 1(\varphi_i)$; on a alors

$$\begin{array}{llll} f_i \psi_i u = 0 & [u \in E_j (j \neq i)] & \text{car déjà} & \psi_i u = 0; \\ f_i \psi_i u = u & (u \in E_i) & \text{car} & f_i \psi_i \equiv 1 \pmod{\varphi_i}. \end{array}$$

Le polynôme $f_i(A) \psi_i(A)$ répond à la question.

ÉTUDE D'UN OPÉRATEUR PRIMAIRE. — Soit A un opérateur primaire de polynôme minimal ψ^α , ψ polynôme premier de R.

THÉOREME 7. — *E_R est somme directe de sous-groupes monogènes isomorphes à $R/(\psi^\beta) (\beta \leq \alpha)$. Le nombre n_β de sous-groupes isomorphes à $R/(\psi^\beta)$ est unique (c'est-à-dire la décomposition est unique à une isomorphie près).*

Pour la démonstration nous aurons besoin de la notion suivante : On appelle *hauteur* $h(u)$ de $u \in E$ et $\neq 0$ la borne supérieure des entiers n tels que $\psi^n v = u$ soit résoluble en v dans E . On n'exclut pas que $h(u) = \infty$, mais ici $\psi^\alpha E = 0$ entraîne que $h(u) < \alpha$.

Posons

$$E_1 = \{ u \in E \mid \psi u = 0 \} \quad \text{et} \quad E_i = \{ u \in E_1 \mid h(u) \geq i-1 \} \quad (i = 1, \dots, \alpha+1).$$

On vérifie que les E_i sont des sous-groupes de E_R et que

$$E_1 \supset E_2 \supset \dots \supset E_\alpha \supset E_{\alpha+1} = 0.$$

$N(E_1)$ est un diviseur de (ψ) puisque $\psi E_1 = 0$; comme ψ est premier on a $N(E_1) = (\psi)$. On peut considérer E_1 comme groupe abélien sur $R/(\psi)$; $R/(\psi)$ étant un corps E_1 est un espace vectoriel. Il existe donc dans E_i des éléments u_i formant une base et tels que

$$E_k = E_{k+1} + \sum_{i \in I_k} (u_i).$$

Dans cette formule il n'est plus nécessaire de préciser si l'on considère E_1 comme groupe abélien sur R ou sur $R/(\psi)$.

Si $i \in I_\lambda$ on a $h(u_i) = k-1$, donc il existe $v_i \in E$ tel que $\psi^{k-1} v_i = u_i$. Nous allons montrer que (première partie du théorème) :

$$E_R = \sum_{i \in I_1} (v_i) + \dots + \sum_{i \in I_\alpha} (v_i) = \sum_i (v_i).$$

La somme est directe. Supposons que $(v_i) \cap (\{v_j \mid j \neq i\}) = F \neq 0$; on a $F \cap E_1 \neq 0$ car si $N(F) = (\psi^\beta)$ on a $\psi^{\beta-1} F \neq 0$ et $\subset E_1$. En remarquant que $(v_i) \cap E_1 = (u_i)$ on obtient $(u_i) \cap (\{u_j \mid j \neq i\}) = F \cap E_1 \neq 0$, ce qui est une contradiction.

Les v_i engendrent E_R . Soit $v \in E$ et $N(v) = (\psi^k)$; on a $\psi^{k-1} v \in E_1$ et comme $h(\psi^{k-1} v) \geq k-1$, on aura

$$\begin{aligned} \psi^{k-1} v &= \sum_{i \in I_k} f_i u_i + \dots + \sum_{i \in I_\alpha} f_i u_i \quad (f_i \in R), \\ \psi^{k-1} v &= \psi^{k-1} \sum_{i \in I_k} f_i v_i + \dots + \psi^{\alpha-1} \sum_{i \in I_\alpha} f_i v_i = \psi^{k-1} v'. \end{aligned}$$

On a $\psi^{k-1}(\nu - \nu') = 0$ ce qui vous ramène à exprimer en fonction des ν_i un élément annulé par ψ^{k-1} . La propriété est démontrée par récurrence.

Soit ν_i tel que $N(\nu_i) = (\psi^\beta)$. D'après le théorème 1 on a $(\nu_i) \cong R/(\psi^\beta)$. Le nombre n_β de sous-groupes (ν_i) isomorphes à $R/(\psi^\beta)$ est la puissance de l'ensemble d'indices I_β ou encore la dimension de $E_\beta/E_{\beta+1}$ considéré comme espace vectoriel sur $R/(\psi)$. On voit que n_β est indépendant de la décomposition, ce qui achève la démonstration du théorème.

Avec Mc Duffee [5] nous dirons que A est un opérateur compagnon du polynôme φ si E_R est monogène et si le polynôme minimal de A est φ ; cela se traduit par $E_R = (u) \cong R/(\varphi)$. On voit que dans (ν_i) , $i \in I_\beta$ l'opérateur induit par A est un opérateur compagnon du polynôme ψ^β .

INVARIANTS DE STRUCTURE D'UN OPÉRATEUR LINÉAIRE. — Des théorèmes 5 et 7 on déduit :

THÉORÈME 8. — Soit A un opérateur linéaire et $\varphi = \psi_1^{z_1} \dots \psi_s^{z_s}$ la décomposition de son polynôme minimal φ en produit de facteurs premiers. A est déterminé à une similitude près par les nombres $n_{i\beta}$ d'opérateurs compagnons des diviseurs primaires ψ_i^β ($\beta = 1, \dots, \alpha_i$; $i = 1, \dots, s$) de φ .

La décomposition de A en somme directe d'opérateurs compagnons des diviseurs primaires de φ est ce qu'on appelle la deuxième forme normale de A . La première forme normale s'obtient en faisant des regroupements : On obtient un opérateur compagnon de φ soit A_1 en faisant une somme directe d'opérateurs compagnons de $\psi_i^{z_i}$ ($i = 1, \dots, s$). On forme ensuite A_2 opérateur compagnon de φ' où φ' est de degré maximum, etc. $\varphi, \varphi', \dots$ sont les diviseurs élémentaires de A . La décomposition $A = A_1 \dot{+} A_2 \dot{+} \dots$ est la première forme normale; c'est elle que l'on obtient quand on utilise la méthode des diviseurs élémentaires.

L'étude de la structure de A est ramenée à l'étude de la structure de l'opérateur compagnon d'un polynôme primaire ψ^β . Un tel opé-

rateur est bien connu puisque alors $E_R \cong R/(\psi^3)$. Par exemple les sous-espaces stables pour A, c'est-à-dire les sous-groupes de E_R , correspondent aux idéaux de R qui divisent (ψ^3) . La suite des diviseurs de (ψ^3) est $(\psi^3) \subset (\psi^{3-1}) \subset \dots \subset (\psi) \subset (1)$. Les sous-espaces de E stables pour A sont donc $0 \subset \psi^{3-1}E \subset \dots \subset \psi E \subset E$. Ce dernier résultat montre que A ne se laisse plus décomposer en somme directe de deux opérateurs.

On dit qu'un opérateur linéaire est non dérogatoire si son polynôme caractéristique $\det(xI - A)$ coïncide avec son polynôme minimal φ . En partant de la deuxième forme normale on voit que cela signifie que les composantes primaires de A ne se laissent plus décomposer, ou encore que A est opérateur compagnon de son polynôme minimal.

III. — Treillis des sous-espaces stables pour un opérateur linéaire.

Un treillis $\mathcal{L}$ est un ensemble partiellement ordonné tel que tout couple d'éléments $a, b \in \mathcal{L}$ possède une borne inférieure : $\inf(a, b)$ et une borne supérieure : $\sup(a, b)$.

L'ensemble des sous-espaces de E stable pour A, c'est-à-dire l'ensemble des sous-groupes de E_R forme un treillis $\mathcal{L}_A$ pour la relation d'inclusion. On a en effet

$$\inf(F, G) = F \cap G, \quad \sup(F, G) = (F, G) \quad (F, G \in \mathcal{L}_A).$$

Le treillis $\mathcal{L}_A$ est distributif si $F, G, H \in \mathcal{L}_A$ entraîne

$$(F, G) \cup H = (F \cap H, G \cap H).$$

Nous verrons que cette propriété caractérise un opérateur non dérogatoire.

$\mathcal{L}_A$ possède un plus petit et un plus grand élément, à savoir zéro et E. Nous dirons que G est un complément de $F \in \mathcal{L}_A$ si $E_R = F + G$; si tout $F \in \mathcal{L}_A$ possède un complément nous dirons que A est *complètement réductible*.

Le produit direct de deux treillis $\mathcal{L}, \mathcal{L}'$ est l'ensemble des couples $(a, a'), a \in \mathcal{L}, a' \in \mathcal{L}'$ ordonné par la relation $(a, a') \leq (b, b')$ si et seulement si $a \leq b, a' \leq b'$, l'égalité n'ayant lieu que si $a = b, a' = b'$. On définit de façon analogue un produit quelconque de treillis. Un produit de treillis distributifs est distributif.

THÉOREME 9. — $\mathcal{L}_A$ est isomorphe au produit direct des treillis $\mathcal{L}_{A_i}$ associés aux composantes primaires $A_1, \dots, A_s$ de A .

Soit $E_R = E_1 + \dots + E_s$ la décomposition obtenue au théorème 5. $\mathcal{L}_{A_i}$ est le treillis des sous-groupes de E_i . Il suffira de montrer que pour tout $F \in \mathcal{L}_A$ on a $F = \sum_{i=1}^s F \cap E_i$. La somme $\Sigma + F \cap E_i$ est bien directe car $\Sigma + E_i$ l'est déjà; comme $F \cap E_i \subset F$ on aura $F \supset \Sigma + F \cap E_i$. Soit $u \in F$ et g_i les polynômes introduits au théorème 6. On a $u = \sum_{i=1}^s g_i u$ avec $g_i u \in E_i$, ce qui achève la démonstration.

THÉOREME 10. — Une condition nécessaire et suffisante pour que A soit non dérogatoire est que $\mathcal{L}_A$ soit distributif.

D'après le théorème 9 il suffit de faire la démonstration dans le cas où A est primaire. Nous reprenons les notations du théorème 5.

Si A est non dérogatoire $\mathcal{L}_A$ est un ensemble fini totalement ordonné, donc est distributif.

Si A est dérogatoire E_1 est un espace vectoriel à plus d'une dimension sur $R/(\psi)$, donc le treillis $\mathcal{L}_1$ des sous-espaces de E_1 n'est pas distributif. $\mathcal{L}_A$ qui prolonge $\mathcal{L}_1$ ne sera pas distributif.

THÉOREME 11. — Une condition nécessaire et suffisante pour que tout élément de $\mathcal{L}_A$ possède un complément est que dans la décomposition du polynôme minimal φ de A en produit de facteurs premiers, tout facteur figure avec l'exposant 1.

La propriété d'existence d'un complément se conservant pour un produit direct de treillis on peut encore se limiter au cas où A est primaire. Soit $\varphi = \psi^\alpha$ où ψ est premier. Si $E_1 = \{u \in E \mid \psi u = 0\}$ est $\neq E$ il n'existe pas $F \in \mathcal{L}_A$ tel que $E = F + E_1$ car si $F \in \mathcal{L}_A$ et $F \not\subset E_1$ on a $F \cap E_1 \neq 0$ [soit $u \in F$, $\notin E_1$ et $N(u) = (\psi^\beta)$; on a $\psi^{\beta-1} u \in F \cap E_1$]. $E = E_1$ est équivalent à $\alpha = 1$; la démonstration s'achève en remarquant que E_1 est un espace vectoriel sur $R/(\psi)$, donc que si $E = E_1$ tout élément de $\mathcal{L}_A$ possède un complément.

CHAPITRE II.

ANNEAUX PARTICULIERS D'OPÉRATEURS LINÉAIRES
SUR UN ESPACE A n DIMENSIONS. PERMUTABILITÉ.

I. — Généralités.

DÉFINITIONS. — Soit E un espace vectoriel quelconque sur un corps commutatif K et $\mathcal{B}$ l'ensemble de tous les opérateurs linéaires sur E . Une partie R de $\mathcal{B}$ est appelée un *anneau d'opérateurs* si :

- (1) $A, B \in R$ entraîne $A - B \in R$;
- (2) $A, B \in R$ entraîne $AB \in R$;
- (3) $A \in R, \lambda \in K$ entraîne $\lambda A \in R$.

Les conditions (1) et (2) sont nécessaires et suffisantes pour que R soit un anneau au sens usuel, mais on a l'habitude de réserver le nom d'anneau d'opérateurs à un ensemble R qui vérifie aussi (3). Un ensemble vérifiant (1), (2), (3) est maintenant souvent appelé une algèbre d'opérateurs; nous conservons l'appellation traditionnelle d'anneau d'opérateurs. Par exemple $\mathcal{B}$ est un anneau d'opérateurs.

Si l'on fait abstraction de la façon dont les opérateurs de R agissent sur E , cela revient à considérer R comme algèbre tout court (sur K), ou ce qui est la même chose comme système hypercomplexe (sur K).

Si $AB = BA$ pour tout $A, B \in R$, R est *commutatif*.

Soit $M, N, \dots$ des parties de $\mathcal{B}$; on note $r(M, N, \dots)$ le plus petit anneau contenant $M, N, \dots$. Par exemple $r(I, A)$ est l'anneau des polynômes en A .

Deux anneaux R et R' sont dits semblables si il existe $S \in GL(E, K)$ tel que $S^{-1}AS$ parcourt R' tout entier lorsque A parcourt R tout entier. Si l'on pose $S^{-1}AS = T(A)$, on a

- (4) $T(A + B) = T(A) + T(B)$ car $S^{-1}(A + B)S = S^{-1}AS + S^{-1}BS$;
- (5) $T(AB) = T(A)T(B)$ car $S^{-1}ABS = S^{-1}ASS^{-1}BS$;
- (6) $T(\lambda A) = \lambda T(A)$ car $S^{-1}\lambda AS = \lambda S^{-1}AS$;
- (7) T est biunivoque car la formule $A' = S^{-1}AS$ est inversible.

Une transformation T vérifiant (4), (5), (6), (7), est un isomor-

phisme des structures de systèmes hypercomplexes de R et R' . Deux anneaux semblables sont donc isomorphes en tant que systèmes hypercomplexes mais la réciproque n'est pas vraie. (On rencontrera des exemples).

L'ANNEAU DES COMMUTANTS D'UN ANNEAU. — Soit R un anneau d'opérateurs linéaires. L'ensemble des opérateurs linéaires qui permutent avec tous ceux de R est un anneau R' que l'on appelle l'anneau des commutants de R .

On peut itérer l'opération $R \rightarrow R'$; on obtient ainsi $R'' \triangleq (R')'$, etc. Si $R \subset S$ cela entraîne $R' \supset S'$; cette remarque jointe à la propriété $R \subset R''$ montre que

$$\begin{aligned} R \subset R'' = R^{IV} = \dots, \\ R' = R''' = R^V = \dots \end{aligned}$$

THÉOREME 12. — Si R est commutatif R'' l'est aussi et l'on a $R \subset R'' \subset R'$.

R commutatif entraîne $R \subset R'$, d'où $R' \supset R''$. D'une façon générale le centre de R est $R \cap R'$; donc ici le centre de R' est $R' \cap R'' = R''$. R'' est commutatif et l'on a $R \subset R'' \subset R'$.

DÉCOMPOSITION D'UN ANNEAU D'OPÉRATEURS. — Soit $E = E_1 + E_2$ où E_1 et E_2 sont deux sous-espaces de E stables pour un anneau R d'opérateurs (c'est-à-dire stables pour tous les opérateurs de l'anneau). Soit R_1 et R_2 les anneaux induits par R dans E_1 et E_2 . Si quels que soient $A_1 \in R_1$, $A_2 \in R_2$ on a $A_1 \nmid A_2 \in R$ on dira que R est somme directe de R_1 et R_2 et l'on écrira $R = R_1 + R_2$.

Soit P la projection sur E_1 parallèlement à E_2 . $R = R_1 + R_2$ entraîne $P \in R'$. Supposons inversement que $P \in R'$, les sous-espaces $E_1 = PE$ et $E_2 = (I - P)E$ sont stables pour R . Tout $A \in R$ s'écrit $A = PA + (I - P)A$, ce qui montre que $R \subset R_1 + R_2$ sans qu'on puisse affirmer l'égalité. On vérifie que R_1 et R_2 sont homomorphes à R , on dit que R est somme sous-directe de R_1 et R_2 .

Si l'on suppose $P \in R \cap R'$, on a $R = R_1 + R_2$, en effet : soit $A_1 \in R_1$, $A_2 \in R_2$; A_1 est la trace sur E_1 de $A \in R$, et A_2 la trace sur E_2 de $B \in R$. On a $A_1 \nmid A_2 = PA + (B - PB) \in R$. Ainsi les projecteurs du centre $R' \cap R$ de R conduisent à des décompositions en somme directe. Il y aura intérêt à les étudier, nous le ferons au prochain paragraphe.

Remarque. — La propriété $R' = R'' = (R'')'$ montre que l'on aura toujours des décompositions simultanées de R et R'' en somme sous-directe.

II. — Treillis de projecteurs.

Ordonnons l'ensemble des projecteurs par la relation « $P \leq Q$ si et seulement si $PQ = QP = P$, $P = Q$ ayant le sens usuel ».

Définition. — Nous dirons qu'une famille $\mathcal{L}$ de projecteurs forme un treillis si :

- (1) $P, Q \in \mathcal{L}$ entraîne $PQ = QP$, $PQ \in \mathcal{L}$, $P \dot{+} Q = P + Q - PQ \in \mathcal{L}$;
- (2) $P, Q \in \mathcal{L}$ et $P \geq Q$ entraîne $P - Q \in \mathcal{L}$.

Les conditions (1) et (2) sont plus qu'il n'en faut pour avoir un treillis au sens strict de ce mot; mais elles sont toujours réalisées dans ce que nous faisons.

On vérifie que $\inf(P, Q) = PQ$ et $\sup(P, Q) = P \dot{+} Q$. Par exemple les projecteurs d'un anneau commutatif forment un treillis.

THÉORÈME 13. — *Un treillis de projecteurs est distributif.*

Il faut vérifier que si $P, Q, S \in \mathcal{L}$, on a

$$\begin{aligned} (P \dot{+} Q)S &= PS \dot{+} QS, \\ (P \dot{+} Q)S &= (P + Q - PQ)S = PS + QS - PQS, \\ PS \dot{+} QS &= PS + QS - PSQS = PS + QS - PQS. \end{aligned}$$

THÉORÈME 14. — *Tout treillis $\mathcal{L}$ de projecteurs sur un espace vectoriel à n dimensions est fini et est engendré par ses projecteurs minimaux $P_1, \dots, P_s$ qui vérifient $P_i P_j = 0$ ($i \neq j$).*

Pour $n = 1$ le théorème est évident. Soit $n > 1$, et $P \in \mathcal{L}$ et $\neq 0$ ou 1. Pour tout $Q \in \mathcal{L}$, on a $Q = PQ + (I - P)Q$, ce qui va permettre d'achever la démonstration par récurrence. Dans PE , $\mathcal{L}$ induit un treillis engendré par $P_1, \dots, P_r$ vérifiant $P_i P_j = 0$ ($i \neq j$) et dans $(I - P)E$, $\mathcal{L}$ induit un treillis engendré par $P_{r+1}, \dots, P_s$ vérifiant $P_k P_l = 0$ ($k \neq l$). On a d'autre part $P_i P_k = 0$ ($i \leq r, k > r$). $\mathcal{L}$ est engendré par $P_1, \dots, P_s$, de façon précise tout projecteur de $\mathcal{L}$ est de la forme $\sum_i \omega_i P_i$ avec $\omega_i = 0$ ou 1. Le plus grand projecteur de $\mathcal{L}$ est $P_1 \dot{+} \dots \dot{+} P_s = P_1 + \dots + P_s$.

III. — Étude des anneaux $r(A)$, $r(I, A)$, $r'(A)$, $r''(A)$.

On suppose maintenant que E est un espace vectoriel à n dimensions sur le corps commutatif K . Soit A un opérateur linéaire sur E , $r(A)$ l'anneau engendré par A , $r(I, A)$ l'anneau des polynômes en A , $r'(A)$ l'anneau des commutants de A . Comme $r(A)$ est commutatif, on a

$$r(A) \subset r(I, A) \subset r''(A) \subset r'(A),$$

$r''(A)$ qui est le centre de $r'(A)$ est aussi commutatif.

Il est pratiquement équivalent d'étudier $r(A)$ ou $r(I, A)$; on a le théorème suivant :

THÉOREME 15. — *Une condition nécessaire et suffisante pour que $r(A) = r(I, A)$ est que A soit inversible.*

Si A est inversible son polynôme minimal $\varphi(x)$ est premier avec x , c'est-à-dire de la forme $a_0 + a_1x + \dots$ avec $a_0 \neq 0$. On en déduit

$$a_0 I = a_0 I - \varphi(A) \in r(A), \quad \text{d'où } I \in r(A).$$

Réciproquement si A n'est pas inversible on ne peut avoir $I = a_1 A + \dots + a_k A^k$ car cela entraînerait que $a_1 I + \dots + a_k A^{k-1}$ serait l'inverse de A .

L'étude de $r(A)$ se fait sans peine en partant des résultats du chapitre précédent sur la structure de A . Nous allons étudier les décompositions de $r(A)$, $r'(A)$, $r''(A)$.

Soit $E_0, E_1, \dots, E_s$ les sous-espaces stables pour A qui correspondent à la décomposition $\varphi = x^\alpha \psi_1^{\alpha_1} \dots \psi_s^{\alpha_s}$ du polynôme minimal de A en facteurs premiers; E_0 correspond au facteur x^α , c'est-à-dire que $E_0 = 0$ si $\alpha = 0$ (A inversible).

D'après le théorème 6 $I_i \in r(I, A)$ ($i = 0, 1, \dots, s$) où I_i est défini par $I_i = 0$ dans E_j ($j \neq i$) et $I_i = I$ dans E_i . On a $I_i \in r(A)$ seulement pour $i = 1, \dots, s$ mais cela suffit pour pouvoir décomposer $r(A)$, $r'(A)$, $r''(A)$ en $r(A) = I_s r(A) + \dots + I_1 r(A)$, etc. Ceci nous ramène au cas où A est un opérateur primaire. Dans ce cas $r(A)$ ne contient plus de projecteurs permettant de pousser plus loin les décompositions, de façon précise, on a :

THÉOREME 16. — *Une condition nécessaire et suffisante pour que A soit primaire est que les seuls projecteurs de $r(I, A)$ soient 0 et 1.*

La condition est suffisante d'après le théorème 6. Pour démontrer la nécessité considérons A primaire de polynôme minimal ψ^α , ψ premier et supposons que $r(I, A)$ contienne un projecteur $P = f(A)$. On a $P(I - P) = 0$, d'où $f(x)[1 - f(x)] \equiv 0 \pmod{\psi^\alpha}$, d'où $f(x)$ ou $1 - f(x) \equiv 0 \pmod{\psi^\alpha}$, d'où $P = 0$ ou $I - P = 0$.

ÉTUDE DE L'ANNEAU $r'(A)$. — Soit A primaire, nous reprenons les notations du théorème 7. Étudier $r'(A)$ c'est étudier l'anneau R' des endomorphismes de E_R . On a $E_R = \sum_i (\varphi_i)$ et $\theta \in R'$ sera déterminé

par la connaissance des $\theta \varphi_i$. La seule condition est que $\theta \varphi_i$ doit engendrer un sous-groupe homomorphe à (φ_i) . Si $i \in I_\beta$, on a $(\varphi_i) \cong R/(\psi^\beta)$; les sous-groupes de (φ_i) sont isomorphes à $R/(\psi^\gamma)$ ($\gamma \leq \beta$); les groupes homomorphes à (φ_i) seront de la forme $(R/(\psi^\beta))/(R/(\psi^\gamma))$ ou en remarquant que $R/(\psi^\gamma) \cong (\psi^{\beta-\gamma})/(\psi^\beta)$ de la forme

$$R/(\psi^{\beta-\gamma}) \cong (R/(\psi^\gamma))/((\psi^{\beta-\gamma})/(\psi^\beta)).$$

Ainsi tout groupe homomorphe à $R/(\psi^\beta)$ est de la forme $R/(\psi^\delta)$ ($\delta \leq \beta$).

Posons $F_k = \{u \in E \mid \psi^k u = 0\}$. F_k est l'ensemble des éléments qui engendrent un groupe homomorphe à $R/(\psi^k)$. On peut choisir $\theta \varphi_i$ ($i \in I_\beta$) arbitrairement dans F_β et ce fait détermine complètement R' . On peut facilement compter le nombre de paramètre dont dépend $r'(A)$.

THÉOREME 17. — *Une condition nécessaire et suffisante pour que A soit non dérogatoire est que $r'(A) = r(I, A)$.*

La nécessité résulte de ce qui précède en remarquant qu'un opérateur de $r(I, A)$ conserve tous les sous-espaces de E stables pour A. La suffisance résulte du théorème 2.

ÉTUDE DE L'ANNEAU $r''(A)$. — **THÉOREME 18.** — *On a $r''(A) = r(I, A)$.*

Nous utiliserons la première forme normale de A et démontrerons le résultat un peu plus général suivant pour le groupe abélien à opérateurs E_R :

THÉOREME 18'. — Si l'on a $E_R = \sum_{i=1}^k (u_i)$ avec $N(u_1) \subset N(u_2) \subset \dots \subset N(u_k)$

tout élément du centre R'' de l'anneau R' des endomorphismes de E_R coïncide avec un élément de R .

Soit $\theta \in R''$ et $\sigma_1, \dots, \sigma_k$ les projections sur $(u_1), \dots, (u_k)$; on a $\sigma_1, \dots, \sigma_k \in R'$ et $\theta\sigma_i = \sigma_i\theta$ montre que $\theta(u_i) \subset (u_i)$. Il existe donc $a_1, \dots, a_k \in R$ avec $\theta u_1 = a_1 u_1, \dots, \theta u_k = a_k u_k$. On a

$$E_R = (u_1 + \dots + u_k) + \sum_{i=2}^k (u_i),$$

en effet : Il est clair que $u_1 + \dots + u_k, u_2, \dots, u_k$ engendrent E_R . Il reste à vérifier que

$$0 = (u_1 + \dots + u_k) \cap \sum_{i=2}^k (u_i);$$

supposons que $b_1(u_1 + \dots + u_k) + b_2 u_2 + \dots + b_k u_k = 0$, cela entraîne $b_1 \in N(u_1), b_1 + b_2 \in N(u_2), \dots, b_1 + b_k \in N(u_k)$ d'où $b_1 \in N(u_1), b_2 \in N(u_2), \dots, b_k \in N(u_k)$ car $N(u_1) \subset N(u_i) (i \geq 2)$. Soit σ la projection sur $(u_1 + \dots + u_k)$; $\sigma\theta = \theta\sigma$ entraîne qu'il existe $a \in R$ avec

$$a(u_1 + \dots + u_k) = \theta(u_1 + \dots + u_k).$$

On a alors

$$\theta(u_1 + \dots + u_k) = au_1 + \dots + au_k = a_1 u_1 + \dots + a_k u_k,$$

d'où

$$au_1 = a_1 u_1, \dots, au_k = a_k u_k.$$

La propriété $\theta u_i = a u_i (i = 1, \dots, k)$ entraîne $\theta = a$ partout, en effet : Soit $v = \sum c_i u_i$, on a

$$\theta v = \sum c_i \theta u_i = \sum c_i a u_i = a \sum c_i u_i = a v.$$

Remarque. — Le théorème démontré peut s'énoncer « $B \in r''(A)$ entraîne $B \in r(I, A)$ ». On a cherché à affaiblir la condition $B \in r''(A)$. H. L. Hamburger [7] a démontré le théorème suivant : Si $B \in r'(A)$ et si B est permutable avec tous les projecteurs de $r'(A)$, on a $B \in r(I, A)$. Si l'on se reporte à la démonstration précédente on voit que nous

avons seulement utilisé l'hypothèse que $B \in r'(A)$ et que B est permutable avec un nombre fini de projecteurs convenablement choisis de $r'(A)$ [qui sont loin d'engendrer l'ensemble de tous les projecteurs de $r'(A)$]. Nous nous sommes d'autre part placés dans un cadre plus général.

IV. — Permutabilité.

$B p. A$ signifie $AB = BA$. Le théorème 17 montre que $B p. A$ n'entraîne pas $B \in r(I, A)$. G. Frobenius [6] posa alors (1896) la question : « Si $B p. A$ existe-t-il C tel que $A \in r(I, C)$, $B \in r(I, C)$? » En 1919 H. B. Phillips donna le contre-exemple suivant :

$$A = \begin{vmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{vmatrix}, \quad B = \begin{vmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{vmatrix}.$$

On a $AB = BA = 0$ et l'on peut vérifier qu'il est impossible de trouver C tel que $A \in r(I, C)$, $B \in r(I, C)$. Nous le démontrerons tout à l'heure sans calcul.

En 1929 K. Shoda [19] énonça le théorème suivant : *Une condition nécessaire et suffisante pour que $A \in r(I, C)$ et $B \in r(I, C)$ est que $r'(A) \supset r'(C)$ et $r'(B) \supset r'(C)$. C'est là une deuxième formulation du théorème 18, en effet : Si $B \in r(I, C)$ il est clair que $r'(B) \supset r'(C)$, si $r'(B) \supset r'(C)$, B est permutable avec tous les opérateurs de $r'(C)$, donc $B \in r''(C) = r(I, C)$. Ceci est d'ailleurs la démonstration de K. Shoda, mais nous ne pouvons considérer ce théorème comme une réponse satisfaisante à la question de G. Frobenius.*

Si la réponse à la question de Frobenius avait été positive cela aurait entraîné que tout anneau commutatif maximal (non contenu dans un anneau commutatif plus grand) engendré par deux opérateurs est de la forme $r(A)$. Un travail de C. Jordan [9] datant de 1905 montre qu'il n'en est pas toujours ainsi. Il est curieux que cela n'ait pas été remarqué. Nous y reviendrons dans le prochain chapitre. Nous allons maintenant étudier plus en détail la permutabilité de deux opérateurs linéaires A et B , afin de répondre en partie à la question de G. Frobenius.

On se ramène en utilisant les résultats du paragraphe précédent au cas d'opérateurs primaires. Nous supposons de plus que K est algé-

briquement clos et de caractéristique nulle; quitte à changer A en $A + \lambda I$ et B en $B + \mu I$ on pourra donc supposer que le polynome minimal de A est x^α , et celui de B, x^β . Il se peut que l'on ait $E = E_1 + E_2$, où E_1 et E_2 sont des sous-espaces stables pour A et B; on a alors $A = A_1 + A_2$, $B = B_1 + B_2$. Supposons que l'on sache trouver C_1 et C_2 tels que $A_1, B_1 \in r(I, C_1)$ et $A_2, B_2 \in r(I, C_2)$. Quitte à changer C_1 en $C_1 + \nu I$ on peut supposer que C_1 et C_2 n'ont pas de valeurs propres communes. On a alors $A, B \in r(I, C_1) + r(I, C_2) = r(I, C)$ [d'après ce qu'on sait des décompositions de $r(C)$, $r'(C)$, $r''(C)$]. Ceci nous montre qu'on peut supposer que A et B ne sont plus simultanément décomposables. Nous le supposons dans ce qui suit.

L'opérateur C cherché est nécessairement non dérogoire car dans le cas contraire on pourrait décomposer C, ce qui conduirait à une décomposition simultanée de A et B. Quitte à changer C en $C + \lambda I$ on peut supposer que $C^n = 0$, n étant la dimension de E. Tous les opérateurs qui interviennent sont maintenant nilpotents.

Nous obtiendrons des conditions nécessaires pour que $A \in r(C)$ en étudiant des propriétés des polynomes en C. Soit $C' = a_1 C + \dots + a_{n-1} C^{n-1}$; pour que $r(C) = r(C')$ il faut et il suffit que $a_1 \neq 0$ car alors

$$C'^{n-1} = a_1^{n-1} C^{n-1} \neq 0 \quad \text{et} \quad C'^n = a_1^n C^n = 0,$$

d'où $\dim r(C) = \dim r(C')$, d'où $r(C) = r(C')$. Nous dirons que C' est un générateur de $r(C)$. Le point de départ de notre étude sera le lemme suivant :

LEMME. — Soit $A = b_i C^i + \dots + b_{n-1} C^{n-1}$ ($b_i \neq 0$); il existe au moins un générateur C' de $r(C)$ tel que $A = b_i C'^i$.

On cherche $C' = C + a_2 C^2 + \dots + a_{n-1} C^{n-1}$ tel que

$$b_i (C + a_2 C^2 + \dots + a_{n-1} C^{n-1})^i = b_i C^i + \dots + b_{n-1} C^{n-1}.$$

En identifiant les coefficients de C , ..., C^{n-1} (qui sont linéairement indépendants) on obtient un système récurrent :

$$\begin{aligned} b_i &= b_i, \\ b_i (i a_2) &= b_{i+1}, \\ b_i \left[\frac{i(i-1)}{2} a_2^2 + i a_3 \right] &= b_{i+2}, \\ &\dots \end{aligned}$$

$a_2, \dots, a_{n-i}$ sont déterminés de façon unique et $a_{n-i+1}, \dots, a_{n-1}$ sont arbitraires.

Ce lemme nous donne un renseignement sur la structure de la suite $n_1, \dots, n_\alpha$ attachée à $A = b_i C^i$. α est le plus petit entier $\geq n/i$. On voit en prenant dans E la base canonique $e_1, \dots, e_n$ ($Ce_1 = 0$, $Ce_2 = e_1, \dots, Ce_n = e_{n-1}$) que tous les n_j ($j = 1, \dots, \alpha$) sont nuls sauf n_α et éventuellement $n_{\alpha-1}$.

Si C' est un générateur de $r(C)$ les sous-espaces de E stables pour C et C' sont les mêmes, à savoir $E \supset CE \supset \dots \supset C^n E = 0$. On a

$$\bar{A}^k(0) = \bar{C}'^k(0) \quad \text{et} \quad A^k E = C'^k E,$$

ce qui montre que $\bar{A}^k(0)$ et $A^k E$ appartiennent à la suite $E, CE, \dots, C^n E$.

On peut résumer comme suit les résultats acquis :

THÉOREME 19. — *Soit A p. B , $A^\alpha = 0$, $B^\beta = 0$, $n_1, \dots, n_\alpha$ les invariants de structure de A , $m_1, \dots, m_\beta$ ceux de B . On suppose A et B non simultanément décomposables. Les conditions suivantes sont nécessaires pour qu'il existe C avec $A, B \in r(C)$:*

$$1^\circ \quad n_1 = \dots = n_{\alpha-2} = m_1 = \dots = m_{\beta-2} = 0;$$

2° Les sous-espaces $\bar{A}^i(0)$, $A^i E$, $\bar{B}^j(0)$, $B^j E$ ($i = 1, \dots, \alpha$; $j = 1, \dots, \beta$) forment un ensemble totalement ordonné par la relation d'inclusion.

Reprenons l'exemple de Phillips; on a $AE = (e_1)$, $BE = (e_2)$ donc C n'existe pas, 2° n'étant pas vérifié. Cet exemple montre de plus que 2° n'est pas une conséquence de B p. A .

L'exemple suivant montre que 1° ne résulte pas non plus de la permutabilité

$$A = \begin{vmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{vmatrix}, \quad B = \begin{vmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{vmatrix}.$$

On a $BA = AB = 0$, $A^3 = 0$, $B^2 = 0$ et l'on vérifie que A et B ne peuvent être décomposés simultanément. Or on a $n_3 = 1$, $n_2 = 0$, $n_1 = 1$.

Nous ne savons pas si les conditions du théorème 19 sont suffisantes.

V. — Anneaux commutatifs complètement réductibles.

Nous dirons qu'un anneau R est complètement réductible si pour tout sous-espace F de E stable pour R , il existe F' stable pour R tel que $E = F + F'$.

En utilisant le treillis des projecteurs d'un anneau commutatif R , on décompose R en une somme directe d'anneaux R_i contenant comme seuls projecteurs zéro et peut-être 1. Le théorème 16 montre que tous les opérateurs d'une composante R_i sont primaires; nous dirons que R_i est un anneau commutatif primaire. Soit R commutatif primaire et $A \in R$ de polynôme minimal ϕ^α , ϕ premier. Le sous-espace $F = \{u \in E \mid \phi u = 0\}$ est stable pour R car si $B \in R$, on a

$$\phi(A)BF = B\phi(A)F = 0,$$

donc $BF \subset F$. Si $\alpha > 1$, F ne permet pas de décomposer A , donc si R est complètement réductible, A aussi.

Inversement soit R commutatif primaire engendré par des opérateurs complètement réductibles. $A \in R$ a un polynôme minimal premier ϕ , donc ou bien $A = 0$ ($\phi \equiv x$) ou bien A est inversible ($\phi \not\equiv x$). R est l'anneau nul ou bien est un corps prolongeant K ($R \neq 0$ entraîne $I \in R$). Dans les deux cas R est complètement réductible (dans le deuxième cas E_R est un espace vectoriel sur R). Finalement on peut énoncer, en tenant compte de ce qu'une extension séparable de K possède toujours un élément primitif :

THÉORÈME 20. — *Une condition nécessaire et suffisante pour qu'un anneau commutatif R soit complètement réductible est que tout $A \in R$ soit complètement réductible. Tout anneau complètement réductible peut*

être décomposé en $R = \sum_{i=1}^s R_i$, où l'un des R_i peut être nul, les autres étant isomorphes à des extensions de K ; si ces extensions sont séparables elles sont engendrées par un seul opérateur.

CAS OU LE CORPS K EST ALGÈBRIQUEMENT CLOS. — Dans ce cas tout opérateur complètement réductible s'écrit $A = 0I_0 + \lambda_1 I_1 + \dots + \lambda_s I_s$ où $I_1, \dots, I_s$ sont les projecteurs de $r(A)$ et $I_0 = I - I_1 - \dots - I_s$.

Nous dirons que A est un opérateur *diagonal*. Un polynome en A s'écrit :

$$P(A) = P(o)1_0 + P(\lambda_1)I_1 + \dots + P(\lambda_s)I_s.$$

THÉORÈME 21. — *Si K est algébriquement clos tout anneau commutatif complètement réductible R est de la forme $r(A)$ où A est un opérateur diagonal.*

Soit $J_1, \dots, J_k$ les projecteurs minimaux de R et $J_0 = I - J_1 - \dots - J_k$.

Tout $B \in R$ s'écrit $B = \sum_{i=1}^k \mu_i J_i$. Considérons $A = \sum_{i=1}^k \lambda_i J_i$ où tous les λ_i

sont différents, ce qui est possible, un corps algébriquement clos ayant une infinité d'éléments. Il nous suffit de montrer qu'il existe un polynome $P(\alpha)$ tel que $P(o) = o$, $P(\lambda_1) = \mu_1$, $\dots$, $P(\lambda_k) = \mu_k$. Un tel polynome s'obtient par exemple par la formule de Lagrange. On a $B = P(A)$.

Remarque 1. — Prenons pour E l'espace unitaire à n dimensions. Le théorème 21 montre que tout anneau commutatif d'opérateurs normaux est toujours engendré par un seul opérateur que l'on peut supposer autoadjoint puisque les λ_i peuvent être choisis réels.

Remarque 2. — La démonstration du théorème 21 montre que les k nombres $n_i = \dim J_i E$ ($i = 1, \dots, k$) constituent un système complet d'invariants de R , relativement à $GL(n, K)$; $n_1, \dots, n_k$ peuvent être fixés arbitrairement, pourvu que $n_1 + \dots + n_k \leq n$. Il existe donc un nombre fini d'anneaux commutatifs complètement réductibles, non semblables, sur un espace à n dimensions.

CHAPITRE III.

ANNEAUX COMMUTATIFS D'OPÉRATEURS SUR UN ESPACE VECTORIEL A n DIMENSIONS.

I. — Anneaux commutatifs d'opérateurs linéaires.

Dans tout ce chapitre, E est un espace vectoriel à n dimensions sur un corps commutatif K et R un anneau commutatif d'opérateurs linéaires sur E .

Nous avons vu que $R \subset R' \subset R''$. Pour les anneaux particuliers étudiés au chapitre précédent on a $R'' = r(R, I)$. Cette propriété n'est plus vraie dans le cas général à partir de $n = 4$, comme nous le montrerons par un exemple.

Nous dirons qu'un anneau commutatif est maximal si $R = R'$, c'est-à-dire n'est pas contenu dans un anneau commutatif plus grand. Un anneau commutatif n'est pas égal à l'intersection des anneaux commutatifs maximaux qui le contiennent, comme le montre le théorème suivant (valable pour E quelconque) :

THÉORÈME 22. — *R'' est l'intersection des anneaux commutatifs maximaux contenant R .*

Soit S commutatif maximal et contenant R ; il faut d'abord montrer que $S \supset R''$. On a $S = S' = S''$; de $S \supset R$ on déduit $S \subset R'$ puis $S \supset R''$.

On a donc $R'' \subset \bigcap_{S_{\max} \supset R} S$ et il reste à vérifier que si $A \notin R''$ il existe S

maximal ne contenant pas A . Deux cas sont à envisager :

1° $R' = R''$ et alors tout anneau commutatif maximal contenant R coïncide avec R'' ;

2° $R' \supset R''$ et alors il existe $B \in R', \notin R''$ et tel que $AB \neq BA$, car dans le cas contraire on aurait $A \in R''$.

Il existe S commutatif maximal prolongeant $r(R'', B)$ qui est commutatif, et nécessairement $A \notin S$ puisque $AB \neq BA$.

En utilisant le treillis des projecteurs de R on décompose R en une somme directe d'anneaux R_i . Les seuls projecteurs de R_i sont zéro et éventuellement 1, donc d'après le théorème 16 tous les opérateurs de R_i sont primaires. On dira que R_i est un anneau commutatif primaire. Un opérateur primaire non inversible étant nilpotent nous pouvons encore dire que dans R_i tout diviseur de zéro est nilpotent. L'étude d'un anneau commutatif est ramenée à l'étude d'un anneau commutatif primaire.

II. — Anneaux commutatifs primaires.

Soit R un anneau commutatif primaire d'opérateurs linéaires. Si $I \notin R$ cela entraîne que tout $A \in R$ est nilpotent [si A inversible $\in R$,

on a $I \in r(A) \subset R]$, ainsi que R puisque R est engendré par un nombre fini d'opérateurs. Comme nous étudierons les anneaux commutatifs nilpotents au prochain paragraphe, nous supposons $I \in R$ dans tout ce qui suit.

Nous allons montrer que lorsque K est un corps parfait l'étude de R primaire peut être ramenée à celle d'un anneau nilpotent. Pour cela nous montrerons que R contient un corps K' isomorphe à un prolongement de K et tel que tout $A \in R$ s'écrive $A = A' + \Lambda$ avec A' nilpotent et $\Lambda \in K'$. On pourra considérer E comme espace vectoriel sur K' , ce qui donnera un nouvel espace E' . On pourra considérer R comme anneau d'opérateurs sur E' et tout $A \in R$ aura alors un polynôme minimal de la forme $(x - \Lambda)^n$ où $\Lambda \in K'$; A s'écrira $A = A' + \Lambda I$, où A' est nilpotent; il suffira d'étudier l'ensemble des opérateurs nilpotents de R , c'est-à-dire un anneau nilpotent. Notons en passant que la propriété pour R d'être maximal est indépendante du fait qu'on considère R comme anneau d'opérateurs sur E ou E' .

Soit N le radical de R , c'est-à-dire dans le cas présent l'ensemble des opérateurs nilpotents de R .

THÉORÈME 23. — *L'anneau R/N est un corps isomorphe à un prolongement de K .*

Première démonstration. — Si $A \in R$ est diviseur de zéro, A n'est pas inversible, donc a la valeur propre zéro, donc est nilpotent. Ainsi il y a identité dans R entre les notions opérateur non inversible, opérateur nilpotent. Dans R/N cela se traduit par l'identité des notions élément non inversible, élément nul. R/N est un corps K' et K' est isomorphe à un prolongement de K car $I \in R$.

Deuxième démonstration. — L'étude d'un anneau commutatif peut être rattachée à la théorie des idéaux de polynômes; les résultats connus peuvent se démontrer par cette voie, mais les méthodes directes semblent en général plus intéressantes. Nous donnons cette démonstration à titre d'exemple.

Soit $R = r(A_1, \dots, A_k)$, on a $R \simeq K[x_1, \dots, x_k]_I Q$ où $K[x_1, \dots, x_k]$ est l'anneau des polynômes de k variables à coefficients dans K et Q l'idéal des polynômes $f(x_1, \dots, x_k)$ qui vérifient $f(A_1, \dots, A_k) = 0$.

Q étant primaire le radical N de R est isomorphe à P/Q, où P est l'idéal premier associé à Q. On a

$$R/N \cong (K[x_1, \dots, x_k]/Q)/(P/Q) \cong K[x_1, \dots, x_k]/P.$$

Soit $\varphi_i(x_i)$ le polynome minimal de A_i . La variété algébrique associée à Q est l'intersection des systèmes d'hyperplans $\varphi_i(x_i) = 0$, c'est-à-dire un système de points conjugués par rapport au corps de base K. P est sans diviseur et $K[x_1, \dots, x_k]/P$ est un corps.

Le théorème 23 est essentiellement le théorème de Dedekind qui dit que tout système hypercomplexe commutatif sans diviseurs de zéro est un corps.

Dans ce qui suit nous identifions K avec le sous-corps isomorphe de $K' = R/N$ en identifiant $\lambda \in K$ avec la classe de λI modulo N.

THÉOREME 24. — *Si K' est un prolongement séparable de K, R contient un corps isomorphe à K' .*

Si K' est séparable sur K, il est de la forme $K[x]/(\psi(x))$ où $\psi(x)$ est un polynome premier séparable de $K[x]$. Il existe alors $A \in R$ tel que $\psi(A) \equiv 0 \pmod{N}$, donc $\psi(A)$ est nilpotent : $\psi^\alpha(A) = 0$. R contient l'anneau $r(A) \cong K[x]/(\psi^\alpha)$ et le théorème 24 sera une conséquence du lemme suivant :

LEMME. — *Si ψ est un polynome premier séparable de $K[x]$, $K[x]/(\psi^\alpha)$ contient un corps isomorphe à $K[x]/(\psi)$.*

Posons $\Sigma = K[x]/(\psi^\alpha)$; le radical Σ^* de Σ est l'ensemble des polynomes $f(x)$ tels que $f^\phi(x) \equiv 0 \pmod{\psi^\alpha}$, donc tels que $f(x) \equiv 0 \pmod{\psi}$. On a $\Sigma^* \cong (\psi)/(\psi^\alpha)$, d'où

$$\Sigma/\Sigma^* \cong (K[x]/(\psi^\alpha))/(\psi)/(\psi^\alpha) \cong K[x]/(\psi).$$

Posons $\Omega = K[x]/(\psi)$ et $\psi(x) = x^q - a_{q-1}x^{q-1} - \dots - a_0$, Ω et Σ sont des systèmes hypercomplexes sur K :

$$\begin{array}{ll} \Sigma = K + K\theta + \dots + K\theta^{q-1} & [\text{table de multiplication } \psi^\alpha(\theta) = 0], \\ \Omega = K + Kz + \dots + Kz^{q-1} & [\text{table de multiplication } \psi(z) = 0]. \end{array}$$

Nous allons montrer que Σ est isomorphe au produit direct $\Omega \times S$ où S est le système hypercomplexe suivant :

$$\begin{aligned} S &= K + K\sigma + \dots + K\sigma^{\alpha-1} \quad (\text{table de multiplication } \sigma^\alpha = 0), \\ \Omega \times S &= \Omega + \Omega\sigma + \dots + \Omega\sigma^{\alpha-1} = K + \dots + Kz^i\sigma^j + \dots + Kz^{q-1}\sigma^{\alpha-1}. \end{aligned}$$

Nous allons montrer que $z + \sigma$ a pour équation minimale $\psi(z + \sigma) = 0$, donc engendre $\Omega \times S$ puisque le rang de ce système est αq . Il en résultera que $z + \sigma \rightarrow \theta$ est un isomorphisme de $\Omega \times S$ sur Σ [les deux systèmes ayant même table de multiplication si l'on prend pour base dans $\Omega \times S$, $1, z + \sigma, \dots, (z + \sigma)^{\alpha q - 1}$].

$$\begin{aligned} \psi(z + \sigma) &= \psi(z) + \sigma\psi'(z) + \sigma^2 h(\sigma, z) && (h \text{ polynome}), \\ &= \sigma\psi'(z) + \sigma^2 h(\sigma, z) && [\text{car } \psi(z) = 0], \\ \psi^\beta(z + \sigma) &= \sigma^\beta \psi'^\beta(z) + \sigma^{\beta+1} g(\sigma, z) && (g \text{ polynome}). \end{aligned}$$

Pour que $\psi^\beta(z + \sigma) = 0$ il faut et il suffit que les coefficients de $\sigma^\beta, \dots, \sigma^{\alpha-1}$ soient nuls (ces coefficients appartiennent à Ω). En particulier il faut que $\psi'^\beta(z) = 0$, c'est-à-dire que $\psi'^\beta(x) \equiv 0 \pmod{\psi}$. Comme ψ et ψ' sont premiers entre eux, cela nécessite $\psi'(x) \equiv 0$, ce qui n'est pas réalisé, $\psi(x)$ étant séparable. Il en résulte que α est le plus petit entier tel que $\psi^\alpha(z + \sigma) = 0$. Soit $g(z + \sigma) = 0$ l'équation de plus bas degré (équation minimale) vérifiée par $z + \sigma$. $g(x)$ divise $\psi^\alpha(x)$, donc $g(x) \equiv \psi^\alpha(x)$ d'après ce qui précède.

$z + \sigma \rightarrow \theta$ est un isomorphisme de $S \times \Omega$ sur Σ . Or $S \times \Omega$ contient le corps Ω , donc Σ contient un corps isomorphe à $\Omega = K[x]/(\psi)$.

CONTRE-EXEMPLE POUR ψ NON SÉPARABLE. — Soit K de caractéristique p et $\psi(x)$ premier non séparable, donc de la forme $\psi(x^p)$.

Supposons que Σ contienne un corps $\Omega \cong K[x]/(\psi)$. On a pour Σ considéré comme espace vectoriel sur K : $\Sigma = \Omega + \Sigma^*$ où Σ^* est le radical de Σ [en effet $\Sigma^* \cap \Omega = 0$ et d'autre part $\text{rang } \Omega + \text{rang } \Sigma^* = q + (\alpha - 1)q = \alpha q = \text{rang } \Sigma$]. Tout élément de Σ s'écrit $\theta = z + \sigma$ avec $z \in \Omega, \sigma \in \Sigma^*$. Prenons pour θ l'élément de Σ qui vérifie l'équation minimale $\psi^\alpha(\theta) = 0$, donc engendre Σ (θ est la classe de x modulo ψ^α). On a $\theta = z + \sigma$ où z vérifie une équation minimale $f(z) = 0$ avec $df^0 \leq d^0 \psi = \text{rang } \Omega$. Le calcul fait plus haut montre que $f^\alpha(z + \sigma) = 0$ ce qui entraîne $\psi^\alpha(x) \equiv f^\alpha(x)$ et par suite $f(x) \equiv \psi(x)$.

On a

$$\psi(z + \sigma) = \psi(z) + \psi(\sigma) - a_0 \quad [a_0 = \psi(0)]$$

car pour $n \neq 0$, on a

$$(z + \sigma)^{p^n} = z^{p^n} + \sigma^{p^n}.$$

Si l'on prend $\alpha \leq p$, on aura $\sigma^p = \sigma^{p^2} = \dots = 0$, donc $\psi(\sigma) = a_0$ et il reste $\psi(z + \sigma) = \psi(z) = 0$, ce qui est une contradiction.

Le théorème 24 est dû essentiellement à J. Wedderburn [25].

Si K est parfait (corps de nombres, corps de Galois) toute extension de K de rang fini est séparable. Dans ce cas l'étude de l'anneau commutatif primaire R pourra être ramenée à celle d'un anneau nilpotent.

III. — Anneaux commutatifs nilpotents.

DÉFINITIONS. — Soit R un anneau commutatif. On dira que R est maximal s'il n'est pas contenu dans un anneau commutatif nilpotent plus grand, ce qui se traduit par $R' = r(R, I)$. On ne connaît à peu près aucun résultat général sur les anneaux commutatifs nilpotents, même maximaux.

R^i désigne l'anneau engendré par les $A_1^{\alpha_1} A_2^{\alpha_2} \dots A_s^{\alpha_s}$ où $A_1, A_2, \dots, A_s \in R$ et $\alpha_1 + \dots + \alpha_s = i$. Si F est un sous-espace de E on pose $R^i(F) = (\{Au \mid A \in R^i, u \in F\})$. On définit ainsi une application $R^i(F)$ de l'ensemble des sous-espaces de E dans lui-même. L'application réciproque sera définie par

$$\bar{R}^i(F) = \{u \in E \mid R^i(u) \subset F\}.$$

Soit ρ le plus petit entier tel que $R^\rho = 0$; ou ce qui est équivalent tel que $\bar{R}^\rho(0) = E$; ρ est l'exposant de R . Les nombres $m_i = \dim \bar{R}^i(0) - \dim \bar{R}^{(i-1)}(0)$ ($i = 1, \dots, \rho$) constituent la signature de R ; cette notion a été introduite par C. Jordan [9]. $m_1, \dots, m_\rho$ sont des invariants de R relativement à $GL(n, K)$, mais pour une signature donnée il peut exister zéro ou plusieurs anneaux. On peut facilement trouver d'autres invariants de R relativement à $GL(n, K)$, par exemple les nombres $\dim R^i(E)$ ($i = 1, \dots, \rho$), les nombres $\dim \bigcap_{A \in R} \bar{A}^i(0)$, etc.

Pour un corps de caractéristique nulle on a cependant :

THÉORÈME 25. — Si K est de caractéristique nulle on a $\bigcap_{A \in R} \bar{A}^i(0) = \bar{R}^i(0)$.

Il est clair que $\bigcap_{A \in R} \bar{A}(o) \supset \bar{R}(o)$; il faut montrer l'inégalité contraire.

En se plaçant dans le sous-espace $\bigcap_{A \in R} \bar{A}(o)$ cela revient à démontrer que « $A^i = o$ quel que soit $A \in R$ » entraîne « $A_1^{\alpha_1} \dots A_s^{\alpha_s} = o$ quel que soit $A_1, \dots, A_s \in R$ et $\alpha_1, \dots, \alpha_s$ pourvu que $\alpha_1 + \dots + \alpha_s = i$ ».

Soit $x_1, \dots, x_s \in K$, on a identiquement en $x_1, \dots, x_s$:

$$o \equiv (x_1 A_1 + \dots + x_s A_s)^i \equiv \sum_{\alpha_1 + \dots + \alpha_s = i} \frac{i!}{\alpha_1! \dots \alpha_s!} x_1^{\alpha_1} \dots x_s^{\alpha_s} A_1^{\alpha_1} \dots A_s^{\alpha_s}.$$

K étant de caractéristique nulle contient une infinité d'éléments, et d'autre part $i! \neq o$; on en déduit $A_1^{\alpha_1} \dots A_s^{\alpha_s} = o$ où $A_1, \dots, A_s \in R$, $\alpha_1 + \dots + \alpha_s = i$.

L'exemple suivant montre que le théorème peut être en défaut si K n'est pas de caractéristique nulle: Soit E un espace à quatre dimensions sur le corps à deux éléments et R l'anneau engendré par les opérateurs

$$A = \begin{vmatrix} o & o & o & o \\ o & o & o & o \\ I & o & o & o \\ o & I & o & o \end{vmatrix}, \quad B = \begin{vmatrix} o & o & o & o \\ I & o & o & o \\ o & o & o & o \\ o & o & I & o \end{vmatrix}.$$

On a

$$R = \{o, A, B, AB, A + B, A + AB, B + AB, A + B + AB\},$$

on vérifie que $A^2 = B^2 = o$, d'où

$$(A + B)^2 = (AB)^2 = (A + AB)^2 = (B + AB)^2 = (A + B + AB)^2 = o,$$

mais on a

$$AB = BA = \begin{vmatrix} o & o & o & o \\ o & o & o & o \\ o & o & o & o \\ I & o & o & o \end{vmatrix} \neq o.$$

On ne connaît pas de systèmes complets d'invariants pour un anneau commutatif nilpotent, même dans le cas où il est maximal et où K est algébriquement clos.

DÉTERMINATION DE TOUS LES ANNEAUX COMMUTATIFS NILPOTENTS MAXIMAUX SUR UN ESPACE VECTORIEL A MOINS DE SIX DIMENSIONS SUR LE CORPS DES NOMBRES COMPLEXES. — Nous allons commencer par un exemple : Déterminer les anneaux commutatifs nilpotents maximaux de signature (1, 2, 3). On est dans un espace à six dimensions sur le corps des nombres complexes. Nous choisirons les vecteurs de base $e_1, \dots, e_6$ comme suit : e_1 dans $\bar{R}(0)$, e_2 et e_3 dans $\bar{R}(0)$. Ces deux conditions seront toujours remplies si l'on change e_2 en $e_2 + e'_2$ avec $e'_2 \in (e_1, e_3)$ ou e_3 en $e_3 + e'_3$ avec $e'_3 \in (e_1, e_2)$ ou e_4 en $e_4 + e'_4$ avec $e'_4 \in (e_1, e_2, e_3, e_5, e_6)$, etc.

Remarquons d'abord que si $A \in R$ on a d'après le théorème 25, $A\bar{R}(0) \subset \bar{R}^{-(l-1)}(0)$. L'exposant de R étant 3 il existe $A \in R$ tel que $A^2 \neq 0$; on peut supposer que $A^2 e_4 \neq 0$ et prendre $e_2 = A e_4$, $e_1 = A e_2$; nécessairement $A e_4 = 0$. Pour $A e_5$ deux cas vont se présenter :

α . Pour tout $e_5 \notin (e_1, e_2, e_3, e_4)$ on a $A e_5 \in (e_1, e_2)$; on se ramène à $A e_5 = 0$; de même on choisira $A e_6 = 0$; si e_3 est choisi arbitrairement on aura $A e_3 = a e_1$ et l'on peut se ramener à $A e_3 = 0$ en changeant e_3 en $e_3 - a e_1$.

β . Il existe e_5 tel que $A e_5 \notin (e_1, e_2)$; on prendra $e_3 = A e_5$ et l'on a $A e_3 = a e_1$; en changeant e_3 en $e_3 - a e_1$ (ce qui nécessite de changer e_5 en $e_5 - a e_4$) on se ramène à $A e_3 = 0$; si $A e_6 = a e_1 + b e_2 + c e_3$ on se ramène à $A e_6 = 0$ en changeant e_6 en $e_6 - a e_1 - b e_2 - c e_3$. On a ainsi les deux possibilités

$$\begin{aligned} (\alpha) \quad & A e_4 = e_2, \quad A e_2 = e_1, \quad A e_1 = A e_3 = A e_5 = A e_6 = 0 ; \\ (\beta) \quad & A e_4 = e_2, \quad A e_2 = e_1, \quad A e_3 = e_3, \quad A e_1 = A e_3 = A e_6 = 0. \end{aligned}$$

Dans le cas α le sous-espace $(e_1, e_3, e_5, e_6) = \bar{A}^{-1}(0)$ est stable pour R et l'anneau induit par R dans $\bar{A}^{-1}(0)$ a pour signature (1, 1, 2). Or il est facile de vérifier qu'il n'existe pas d'anneau de signature (1, 1, 2) ; on pourra pour cette question se rapporter à C. Jordan [9].

Donc on est nécessairement dans le cas β . D'après le théorème 25 il existe $B \in R$ tel que $B^2 e_6 \neq 0$. On a $B^2 e_6 = \lambda e_1$ et en changeant B en $\sqrt{\lambda} B$ on peut supposer que $B^2 e_6 = e_1$. On a $B e_6 = a_1 e_1 + a_2 e_2 + a_3 e_3$; en changeant B en $B - a_1 B^2$ on peut supposer $a_1 = 0$; $AB = BA$ entraîne $a_2 = 0$; enfin en changeant e_5 en $a_3 e_3$, e_3 en $a_3 e_3$, ce qui ne modifie pas β , on aura $B e_6 = e_3$, $B e_3 = e_1$. La condition $AB = BA$

montre encore que $Be_3 = e_2$, $Be_4 = Be_2 = 0$. Considérons l'anneau

$$R = r(A, B) = r\left(\left(\begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right), \left(\begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{array}\right)\right).$$

R est commutatif nilpotent de signature $(1, 2, 3)$. R est maximal car nous verrons plus loin qu'un anneau de signature $(1, m_2, m_3, \dots, m_p)$ est maximal. Il en résulte que R est le seul anneau de signature $(1, 2, 3)$.

C. Jordan [9] a étudié un certain nombre de signatures, ce qui lui a permis de déterminer tous les anneaux commutatifs maximaux sur un espace vectoriel à moins de sept dimensions sur le corps des nombres complexes. Le Mémoire de Jordan contient quelques erreurs ; par exemple Jordan indique sept anneaux de signature $(1, 2, 3)$ alors qu'il y en a seulement un comme nous venons de le voir.

D'autre part Jordan ne donne pas de formes réduites pour les anneaux de signature donnée, mais se contente de déterminer leur nombre. Nous pensons donc utile de donner des formes réduites pour les anneaux commutatifs nilpotents maximaux sur un espace à moins de six dimensions sur le corps des nombres complexes. Cela nous fournira des exemples intéressants ; nous ne faisons pas de démonstrations.

Signature $(1, 1)$:

$$(1) \quad R = r\left(\begin{array}{cc} 0 & 0 \\ 1 & 0 \end{array}\right).$$

Signature $(1, 1, 1)$:

$$(2) \quad R = r\left(\begin{array}{ccc} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{array}\right).$$

Signature $(2, 1)$:

$$(3) \quad R = r\left(\begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{array}, \begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{array}\right).$$

Signature $(1, 2)$:

$$(4) \quad R = r\left(\begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{array}, \begin{array}{ccc} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right).$$

Signature (1, 1, 1, 1, 1):

$$(12) \quad R = r \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Signature (1, 1, 1, 2) : Rien.

Signature (1, 1, 2, 1) : Rien.

Signature (1, 2, 1, 1) :

$$(13) \quad R = r \left(\begin{array}{c|c} \begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array} & \begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \end{array} \right);$$

$$(14) \quad R = r \left(\left[\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array} \right], \left[\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{array} \right] \right).$$

Signature (2, 1, 1, 1):

$$(15) \quad R = r \left(\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array} \right), \quad \begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{array} \right).$$

Signature (1, 1, 3): Rien.

Signature (1, 3, 1) :

$$(16) \quad R = r \left(\begin{vmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{vmatrix}, \begin{vmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{vmatrix}, \begin{vmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{vmatrix} \right);$$

$$(17) \quad R = r \left(\begin{array}{c|c|c} \begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{array} & \begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{array} & \begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array} \end{array} \right);$$

Il est facile de constater la non-similitude des anneaux correspondant à une même signature. Pour être complet nous démontrerons au prochain paragraphe la maximalité des anneaux (1) à (29).

EXEMPLES D'OPÉRATEURS PERMUTABLES NON FONCTIONS D'UN MÊME TROISIÈME. — Si A p. B entraînait l'existence de C tel que $A, B \in r(I, C)$ nous avons vu qu'il en résulterait que tout anneau commutatif maximal engendré par deux opérateurs serait de la forme $r(C)$. Parmi les anneaux (1) à (29), 12 sont engendrés par deux opérateurs.

STRUCTURE DES ANNEAUX COMMUTATIFS NILPOTENTS. — Nous avons déjà dit qu'on ne connaît pas de système complet d'invariants pour un anneau commutatif nilpotent. On ne sait même pas s'il existe un nombre fini de tels anneaux sur un espace à n dimensions sur le corps des nombres complexes. Dans les exemples donnés on a toujours pu trouver une base de E et un système de générateurs pour R qui transforment un vecteur de base en un autre vecteur de base. Si ce fait était général, il entraînerait qu'il n'existe qu'un nombre fini d'anneaux commutatifs nilpotents sur un espace à n dimensions.

Nous suggérons aussi que l'on pourrait faire intervenir systématiquement l'ensemble $\mathcal{L}$ des sous-espaces invariants par similitude (pour tout S tel que $R = S^{-1}RS$). Nous avons constaté sur des exemples que $\mathcal{L}$ était fini, mais nous n'avons pu obtenir de résultats généraux.

Les exemples étudiés montrent qu'un anneau commutatif maximal sur un espace à n dimensions dépend de n paramètres au moins. Nous ne savons pas si ce fait est général. J. Schur [20] a montré que le nombre de paramètres est $\leq 1 + [n^2/4]$ ($[]$ désigne la partie entière). Pour $n \geq 4$ les anneaux correspondant à ce maximum sont de la forme $r(R, I)$ où R est du type (10) si n est pair et du type (28) ou (29) si n est impair. N. Jacobson [8] a montré que ces résultats sont valables avec un corps commutatif quelconque (J. Schur prenait le corps des nombres complexes). M. F. Kravcuk [11] a étudié les anneaux d'exposant ρ fixé et dépendant du nombre maximum possible de paramètres ; un exemple est l'anneau (20).

IV. — Relations avec les systèmes hypercomplexes commutatifs. Applications.

REPRÉSENTATION RÉGULIÈRE D'UN SYSTÈME HYPERCOMPLEXE. — 1° *Système*

hypercomplexe avec élément unité. — Soit Σ un système hypercomplexe de rang n sur le corps K . Considéré comme groupe abélien sur K , Σ est un espace vectoriel à n dimensions que nous appellerons E et dont les éléments seront notés par les mêmes lettres (petites) que ceux de Σ .

A tout $a \in \Sigma$ on peut faire correspondre un opérateur linéaire sur E , que nous noterons A , défini par

$$Au = au \quad (u \in E),$$

Σ ainsi envisagé est un anneau R d'opérateurs linéaires sur E appelé représentation régulière gauche de Σ . Cette représentation est fidèle car $A = 0$ entraîne $A1 = a = 0$. E considéré comme groupe abélien sur R est monogène car $E = R1$. Cette propriété caractérise l'ensemble des représentations équivalentes à la représentation régulière, en effet : Si S est équivalente à R , c'est-à-dire si $S = P^{-1}RP$, on a $E = SP^{-1}1$. Si inversement S est une représentation de Σ dans E telle que $E = S\varphi$ il existe P tel que $S = P^{-1}RP$: R et S sont isomorphes à Σ , en tant que systèmes hypercomplexes ; mais les conditions $E = R1 = S\varphi$ entraînant que R et S sont de rang n , ils seront isomorphes à Σ et par suite isomorphes entre eux. Soit alors T un isomorphisme des structures de système hypercomplexe de R et S , et P l'opérateur linéaire défini par $T(A)1 = PA\varphi$, $A \in R$. Lorsque A parcourt R , $A\varphi$ parcourt E , ainsi que $T(A)1$, donc P est inversible. Soit $A, B \in R$, on a

$$T(A)T(B)1 = T(AB)1 = PAB\varphi = PAP^{-1}T(B)1 ;$$

comme $T(B)1$ parcourt E , on aura $T(A) = PAP^{-1}$ et tout est démontré.

2° *Système hypercomplexe sans élément unité.* — La représentation régulière n'est plus fidèle, mais il est facile d'obtenir une représentation fidèle. Pour cela nous considérerons avec J. H. M. Wedderburn le système $\Sigma^0 = K + \Sigma$ obtenu en adjoignant à Σ un élément unité, et nous prendrons pour E l'espace vectoriel Σ^0 . On définit R en faisant correspondre à tout $a \in \Sigma$ l'opérateur A tel que $Au = au$, $u \in E$, cette représentation peut être considérée comme induite par la représentation régulière de Σ^0 . Dans le cas présent E considéré comme groupe

abélien sur $p(R, I)$ est monogène et l'on vérifie comme plus haut que cette propriété caractérise l'ensemble des représentations équivalentes à R .

Pour la commodité du langage nous appellerons représentation canonique de Σ la représentation régulière gauche si Σ contient 1 , la représentation induite par la représentation régulière gauche de $\Sigma^0 = K + \Sigma$ si $1 \notin \Sigma$.

La propriété « $E_{r(R, I)}$ est monogène » caractérise l'ensemble des représentations équivalentes à la représentation canonique, de sorte que l'étude des systèmes hypercomplexes peut se déduire de l'étude des anneaux d'opérateurs tel que $E_{r(R, I)}$ est monogène.

SYSTÈMES HYPERCOMPLEXES COMMUTATIFS DE RANG < 5 SUR LE CORPS DES NOMBRES COMPLEXES. — Soit Σ un système hypercomplexe commutatif contenant 1 , R sa représentation canonique. De $E = R1$ on déduit (théorème 2) que $R' = R$ (cela résulte aussi de ce que R' est la représentation régulière droite). R est donc commutatif maximal.

Si R se décompose en une somme directe de deux anneaux d'opérateurs : $R = R_1 + R_2$, c'est *a fortiori* une décomposition de R considéré comme système hypercomplexe. Donc finalement il suffit de déterminer les systèmes hypercomplexes commutatifs nilpotents; on les obtiendra à partir de leur représentation canonique, c'est-à-dire à partir des anneaux commutatifs nilpotents vérifiant la condition $\mu_1 = \text{codim } RE = 1$. Les anneaux vérifiant cette condition sont (1), (2), (3), (5), (7), (8), (11), (12), (14), (15), (16), (19), (21), (22), (23), (26). Tous ces anneaux sont indécomposables en tant qu'anneaux d'opérateurs linéaires, mais seuls (1), (2), (5), (7), (12), (14), (16), (22) sont des systèmes hypercomplexes indécomposables (nous reviendrons sur ce fait dans un instant). Nous donnons une table de multiplication pour chacun de ces systèmes :

Rang 1 :

$$\begin{array}{c|c} & a \\ \hline a & 0 \end{array}$$

Rang 2 :

$$\begin{array}{c|cc} & a & b \\ \hline a & b & 0 \\ b & 0 & 0 \end{array}$$

Rang 3 :

	a	b	c		a	b	c
a	b	c	0	a	c	0	0
b	c	0	0	b	0	c	0
c	0	0	0	c	0	0	0

Rang 4 :

	a	b	c	d		a	b	c	d
a	b	c	d	0	a	b	c	0	0
b	c	d	0	0	b	c	0	0	0
c	d	0	0	0	c	0	0	0	0
d	0	0	0	0	d	0	0	0	0
	a	b	c	d		a	b	c	d
a	b	0	d	0	a	d	0	0	0
b	0	0	0	0	b	0	d	0	0
c	d	0	0	0	c	0	0	d	0
d	0	0	0	0	d	0	0	0	0

DÉCOMPOSITION D'UN ANNEAU COMMUTATIF D'OPÉRATEURS, CONSIDÉRÉ COMME SYSTÈME HYPERCOMPLEXE. — Soit R commutatif nilpotent et $R = R_1 + R_2$ une décomposition de R considéré comme système hypercomplexe. Cela signifie que $RR_1 \subset R_1$, $RR_2 \subset R_2$, $R_1 \cap R_2 = 0$; on en déduit $R_1 R_2 \subset R_1 \cap R_2 = 0$.

Définition 1. — Nous dirons qu'un sous-espace $E_1 \subset E$ est un support de la composante R_1 si $R_1 E = R_1 E_1 \subset E_1$, nous dirons que E_1 est minimal si il ne contient pas de support plus petit.

On peut construire un support minimal de R_1 comme suit : soit F un sous-espace supplémentaire de $R_1 E \cap \bar{R}_1^{-1}(0)$ dans $\bar{R}_1^{-1}(0)$. On prendra E_1 tel que $E_1 \supset R_1 E$, $E_1 + F = E$.

Définition 2. — Nous dirons que $u \in E_1$ est initial pour R_1 si $u \notin R_1 E$ et que u est terminal pour R_1 si $u \in \bar{R}_1^{-1}(0)$.

THÉOREME 26. — Soit $R = R_1 + R_2$, E_1 et E_2 des supports minimaux de R_1 et R_2 respectivement. Si $u \in E_1 \cap E_2$, u est initial pour R_1 et R_2 ou terminal pour R_1 et R_2 .

Supposons u non initial pour R_1 ; cela signifie qu'il existe $A_1 \in R_1$ et $v \in E_1$ avec $u = A_1 v$. De $R_1 R_2 = 0$ résulte $R_2 A_1 v = R_2 u = 0$, ce qui montre que u est terminal pour R_2 . D'après la condition de minimalité des supports un vecteur ne peut être à la fois initial et terminal pour R_1 , donc u est non initial pour R_2 et par suite terminal pour R_1 . Il reste comme possibilités u initial pour R_1 et R_2 ou u terminal pour R_1 et R_2 .

Exemples. — Reprenons les anneaux (3) et (4) en désignant par e_1, e_2, e_3 les vecteurs de base et par A et B les opérateurs. Pour (3) on a $R = r(A) + r(B)$ où le signe $+$ désigne une somme directe au sens système hypercomplexe. On peut prendre pour supports $E_1 = (e_1, e_3)$, $E_2 = (e_2, e_3)$, on a $E_1 \cap E_2 = (e_3)$ et e_3 est initial pour $r(A)$ et $r(B)$. Pour l'anneau (4) on vérifie que les supports se coupent suivant des vecteurs terminaux pour $r(A)$ et $r(B)$. Les anneaux (3) et (4) se correspondent par dualité.

Nous allons montrer par deux applications que les notions précédentes peuvent être utiles pour l'étude de la structure des anneaux commutatifs d'opérateurs linéaires.

PREMIÈRE APPLICATION : UN CRITÈRE DE MAXIMALITÉ. — THÉORÈME 27. — Soit R un anneau commutatif nilpotent d'opérateurs linéaires, $R = R_1 + \dots + R_s$ une décomposition de R considéré comme système hypercomplexe, $E_1, \dots, E_s$ des supports de $R_1, \dots, R_s$ respectivement, que l'on suppose vérifier les conditions :

$$(1) \quad E_i \cap \bar{R}_i^{-1}(0) = E_i \cap F_i, \quad \text{où } F_i = (\{ E_j \mid j \neq i \}) ;$$

$$(2) \quad \bar{R}_i^{-1}(0) = F_i.$$

Si chaque R_i considéré comme anneau d'opérateurs sur E_i est maximal, il en est de même de R .

On a $E_i = \bigcap_{j \neq i} F_j = \bigcap_{j \neq i} \bar{R}_j^{-1}(0)$, ce qui montre que E_i est stable pour tout $A \in R'$. Dans le sous-espace E_i on peut écrire $A = \lambda_i I + A_i$ où $\lambda_i \in K$, $A_i \in R_i$. Dans le sous-espace $\bar{R}^{-1}(0) = \bigcap_i F_i = \bigcap_i E_i = E_j \cap \bar{R}_j^{-1}(0)$, on a $A = \lambda_1 I = \dots = \lambda_s I_s$, ce qui montre que tous les λ_i sont égaux. D'après la définition du support d'une composante, on a

$E = (E_i, F_i) = (E_1, \dots, E_s)$; comme d'autre part $A_i E_j = 0$ si $i \neq j$, on en déduit $A = \lambda_1 I + A_1 + \dots + A_s$, ce qui démontre la maximalité de R .

Pour pouvoir utiliser le théorème précédent il faut déjà connaître des types d'anneaux commutatifs maximaux. Nous allons indiquer deux types simples.

Type I. — Anneaux commutatifs nilpotents tels que $E_{\nu(R, I)}$ soit monogène. Comme nous l'avons déjà remarqué la maximalité de ces anneaux résulte du théorème 2; ils sont caractérisés par $\mu_1 = \text{codim } RE = 1$.

Type II. — Anneaux commutatifs nilpotents tels que

$$m_1 = \dim \bar{R}^1(0) = 1.$$

Le type II se déduit par dualité du type I, en effet : Soit E' l'espace des formes linéaires sur E , $\langle u, u' \rangle$ la valeur de la forme linéaire u' pour $u \in E$. A chaque opérateur linéaire A correspond son transposé A^* défini par $\langle Au, u' \rangle = \langle u, A^*u' \rangle$.

A un anneau R correspond un anneau R^* inversement isomorphe : $(A + B)^* = A^* + B^*$, $(\lambda A)^* = \lambda A^*$, $(AB)^* = B^*A^*$. Si R est commutatif R et R^* seront isomorphes, mais non nécessairement semblables [parmi les anneaux (1) à (29) ceux qui sont semblables à l'anneau transposé sont (1), (2), (5), (7), (10), (12), (16)]. Supposons maintenant R commutatif nilpotent. Si R est maximal il en est de même de R^* , de sorte que la maximalité des anneaux du type II sera une conséquence du lemme suivant :

LEMME. — $\dim \bar{R}^1(0) = \text{codim } R^*E' \text{ (ou } m_1 = \mu'_1)$.

Il suffit de montrer que $\bar{R}^1(0)$ est le sous-espace orthogonal à R^*E' . Soit $u \in \bar{R}^1(0)$, on a $\langle u, A^*u' \rangle = \langle Au, u' \rangle = 0$, ce qui montre que $u \perp R^*E'$. Soit $u \perp R^*E'$, on a $\langle u, A^*u' \rangle = \langle Au, u' \rangle = 0$ quels que soient $u' \in E'$, $A \in R$ donc $Au = 0$ pour tout $A \in R$, donc $u \in \bar{R}^1(0)$.

On peut vérifier que le théorème 28 permet de démontrer la maximalité de tous les anneaux (1) à (29). Il permet aussi de recon-

naître la maximalité des anneaux étudiés par J. Schur [20] et M. F. Kravcuk [11].

DEUXIÈME APPLICATION : UN EXEMPLE GÉNÉRAL D'ANNEAU COMMUTATIF TEL QUE $R'' \neq r(R, I)$. — Soit R un anneau commutatif nilpotent d'opérateurs linéaires, $R = R_1 + R_2$ une décomposition de R considéré comme système hypercomplexe, E_1 et E_2 des supports de R_1 et R_2 respectivement.

On obtient un anneau tel que $R'' \neq r(R, I)$ si l'on suppose remplies les conditions suivantes :

- (1) $R_1 E_2 = R_2 E_1 = 0$;
- (2) $\bar{R}_2^1(0) \cap E_2 = \bar{R}_1^1(0), \quad \bar{R}_1^1(0) \cap E_1 \subset \bar{R}^1(0)$;
- (3) R_1 et R_2 sont maximaux dans les sous-espaces E_1 et E_2 respectivement.

Nous allons déterminer R' . Pour cela posons $E'_1 = (E_1, \bar{R}^1(0))$ et soit $u_1, \dots, u_\alpha$ tels que $E_1 = R_1 E_1 + (u_1) + \dots + (u_\alpha)$, $v_1, \dots, v_\beta$ tels que $E'_1 = E_1 + (v_1) + \dots + (v_\beta)$. Soit A_{ij} l'opérateur linéaire défini par

$$A_{ij} u_k = \delta_{ik} v_j \quad (\delta_{ik}, \text{ symbole de Kroneker}),$$

$$A_{ij} R_1 E_1 = A_{ij} E_2 = 0.$$

Remarquons que $E = (E_1, E_2)$, cela résulte de ce que (E_1, E_2) est un support de l'anneau R et de l'hypothèse (2) qui entraîne $\bar{R}^1(0) \subset (E_1, E_2)$. Nous allons en déduire que $E_2 = \bar{R}_1^1(0)$, $E'_1 = \bar{R}_2^1(0)$, ce qui montrera que E'_1 et E_2 sont stables pour tout $A \in R'$. D'après (2) on a $E_2 \subset \bar{R}_1^1(0)$; supposons que l'on ait $R_1 u = 0$ avec $u \notin E_2$, on peut écrire $u = u_1 + u_2$ avec $u_1 \in E_1$, $u_1 \notin E_2$, $u_2 \in E_2$, d'où $R u_1 = 0$ ce qui contredit (2). On a $E_2 = \bar{R}_1^1(0)$ et l'on voit de façon analogue que $E'_1 = \bar{R}_2^1(0)$. Dans E_2 on a $A = \lambda_2 I + A_2$ où $A_2 \in R_2$. Dans E'_1 on a $A = A'_1 \in S =$ anneau des commutants de R_1 considéré comme anneau d'opérateurs sur E'_1 . D'après la définition des A_{ij} on peut former $B = A'_1 + \sum_{j=1}^{\beta} a_{ij} A_{ij}$ tel que $B u_i \in E_1$ ($i = 1, \dots, \alpha$). De $B \in S$ résulte alors $B E_1 \subset E_1$, en effet : D'après la définition des u_i tout $u \in E_1$ s'écrit

$u = \sum_i B_i u_i$ où $B_i \in p(R_1, I)$; on en déduit

$$Bu = \sum_i BB_i u_i = \sum_i B_i B u_i \subset E_1.$$

On a donc

$$B = \lambda_1 I + A_1, \quad \text{où } A_1 \in R_1.$$

Dans le sous-espace $\bar{R}(0)$ on a $A = \lambda_1 I = \lambda_2 I$, ce qui montre que $\lambda_1 = \lambda_2$, d'où finalement en tenant compte de $A_1 E_2 = A_2 E'_1 = 0$:

$$A = \lambda_1 I + A_1 + A_2 + \sum_{ij} a_{ij} A_{ij} \in r(R, A_{11}, \dots, A_{\alpha\beta}, I) = R'.$$

Comme R' est commutatif on aura également :

$$R'' = r(R, A_{11}, \dots, A_{\alpha\beta}, I) \neq r(R, I).$$

L'exemple le plus simple d'anneau commutatif vérifiant (1), (2) et (3) s'obtient dans le cas d'un espace à quatre dimensions. Soit A, B, C, D les quatre opérateurs de l'anneau (10). Si l'on pose $R = r(A, B, C)$, on a

$$R = r(C) + r(A, B) = R_1 + R_2.$$

Les sous-espaces $E_1(e_1, e_3)$, $E_2(e_1, e_2, e_4)$ sont des supports de R_1 et R_2 tels que (1), (2), (3) sont vérifiés. On a $E'_1 = (e_1, e_2, e_3)$, donc

$$R'' = r(A, B, C, D, I) \neq r(R, I).$$

Il est facile de vérifier que dans le cas d'un espace à trois dimensions on a toujours $R'' = r(R, I)$, donc l'exemple précédent est le plus simple.

CHAPITRE IV.

OPÉRATEURS LINÉAIRES SUR UN ESPACE VECTORIEL QUELCONQUE.

Soit E un espace vectoriel sur un corps commutatif K et A un opérateur linéaire sur E . Nous avons vu que l'étude de A à une similitude près était équivalente à l'étude du groupe abélien à opérateurs $E_{K[x]}$.

L'étude du cas général n'est pas autre chose que l'étude des groupes

abéliens quelconques. Nous nous limiterons surtout aux deux cas particuliers suivants :

1° $E_{K[x]}$ est un groupe abélien de torsion, c'est-à-dire tout $u \in E$ a un annulateur $\neq 0$. Si l'on veut on pourra dire que A est un opérateur de torsion.

2° $E_{K[x]}$ est un groupe cyclique généralisé, c'est-à-dire tout sous-groupe de $E_{K[x]}$ ayant un nombre fini de générateurs est monogène ; on dit encore que $E_{K[x]}$ est de rang 1. Nous verrons que la plupart des propriétés des opérateurs non dérogoires sont encore valables, de sorte que nous pourrions dire que A est non dérogoire si $E_{K[x]}$ est de rang 1.

Nous emploierons uniquement le langage des groupes abéliens à opérateurs. Nous traduirons seulement quelques résultats pour l'opérateur linéaire A (cela ne représente aucune difficulté).

I. — Considérations générales.

Soit E un groupe abélien muni d'un anneau R d'opérateurs avec les conditions :

- 1° R est commutatif, sans diviseurs de zéro et possède un élément unité ;
- 2° Tout idéal de R est principal ;
- 3° L'unité de R est opérateur unité.

L'ensemble des endomorphismes de E sera noté R' , le centre de R' sera noté R'' . Comme R est commutatif tout $a \in R$ définit un endomorphisme de E et l'on a $R \subset R'' \subset R'$ (quand nous considérons R comme anneau d'endomorphismes nous identifions les éléments de R qui définissent le même endomorphisme).

LA TOPOLOGIE FINIE SUR R' . — Soit S l'ensemble des applications de E dans E ; S devient un groupe abélien à opérateurs si l'on pose

$$\begin{aligned} (\theta + \sigma) u &= \theta u + \sigma u & (\theta, \sigma \in S; u \in E); \\ (a\theta) u &= a(\theta u) & (\theta \in S; a \in R; u \in E). \end{aligned}$$

Il est commode de munir S de la topologie finie (topologie de la

convergence simple, E étant considéré comme muni de la topologie discrète) définie par le système fondamental de voisinages de zéro :

$$W_{u_1, \dots, u_n} = \{ \theta \in S \mid \theta u_1 = \dots = \theta u_n = 0 \},$$

$\{u_1, \dots, u_n\}$ parcourt l'ensemble des parties finies de E.

La fermeture d'une partie T de S sera notée $\bar{T}$.

THÉOREME 28. — Soit $(v_1, \dots, v_n) \rightarrow f(v_1, \dots, v_n)$ une application de $E \times \dots \times E$ dans E. L'ensemble T des $\theta \in S$ qui vérifient la relation $f(\theta u_1, \dots, \theta u_n) = 0$, où $u_1, \dots, u_n$ sont n éléments arbitraires de E est fermé dans S.

Soit $u_1, \dots, u_n \in E$ et $\sigma \in \bar{T}$; il existe $\theta \in T$ tel que $\theta - \sigma \in W_{u_1, \dots, u_n}$ donc

$$f(\sigma u_1, \dots, \sigma u_n) = f(\theta u_1, \dots, \theta u_n) = 0.$$

COROLLAIRE 1. — R' est fermé dans S.

R' est l'ensemble des $\theta \in S$ qui vérifient les relations

$$(4) \quad \theta(u + v) - \theta u - \theta v = 0;$$

$$(5) \quad \theta(au) - a(\theta u) = 0.$$

La relation (4) fait intervenir trois éléments : $u + v$, u , v et la relation (5) deux éléments : u , au .

COROLLAIRE 2. — $\bar{R} \subset R''$.

Pour que $\theta \in R''$ il faut que pour tout $\sigma \in R'$ on ait $\theta(\sigma u) - \sigma(\theta u) = 0$, cette relation fait intervenir deux éléments de E : u , σu .

On a donc

$$R \subset R \subset R'' \subset R'.$$

LE THÉOREME FONDAMENTAL SUR LES GROUPES ABÉLIENS A OPÉRATEURS. — On peut énoncer ce théorème comme suit : Soit E un groupe abélien à opérateurs vérifiant les conditions (1), (2), (3). Tout sous-groupe de E ayant un nombre fini de générateurs est somme directe de groupes monogènes.

Une conséquence de ce théorème est :

THÉOREME 29. — Soit E un groupe abélien à opérateurs vérifiant les

conditions (1), (2), (3). $\bar{R}$ coïncide avec le sous-ensemble R^* des endomorphismes de E qui laissent invariants tous les sous-groupes de E .

On a $\bar{R} \subset R^*$, en effet : Si l'endomorphisme θ appartient à $\bar{R}$ on a pour tout $u \in E$ $\theta u = au$ avec $a \in R$. θ conserve tous les sous-groupes monogènes de E , et par suite tous les sous-groupes de E , c'est-à-dire $\theta \in R^*$.

On a $R^* \subset \bar{R}$, en effet : Soit $\theta \in R^*$; il faut montrer que pour tout système fini $u_1, \dots, u_n$ d'éléments de E il existe $a \in R$ tel que $\theta u_i = au_i$ ($i = 1, \dots, n$). Par hypothèse on a

$$(u_1, \dots, u_n) = (v_1) + \dots + (v_k),$$

où le deuxième membre est une somme directe. Comme $\theta \in R^*$, on a

$$\begin{aligned} \theta v_1 &= a_1 v_1, & \dots, & & \theta v_k &= a_k v_k, \\ \theta(v_1 + \dots + v_k) &= a(v_1 + \dots + v_k), & \text{avec} & & a_1, \dots, a_k &\in R \end{aligned}$$

On a

$$\theta(v_1 + \dots + v_k) = a(v_1 + \dots + v_k) = a_1 v_1 + \dots + a_k v_k,$$

d'où

$$a_i v_i = a v_i \quad (i = 1, \dots, k).$$

Soit alors $v \in (u_1, \dots, u_n)$, on peut écrire $v = \sum b_i v_i$ avec $b_i \in R$. Il vient

$$\theta v = \theta \sum b_i v_i = \sum b_i \theta v_i = \sum b_i a v_i = a \sum b_i v_i = a v,$$

ce qui achève la démonstration.

GROUPES ABÉLIENS DE TORSION. — Un groupe abélien E à opérateurs sera dit un groupe abélien de torsion si en plus des conditions (1), (2), (3) il vérifie la condition :

(4) Tout $u \in E$ a un annulateur $\neq 0$.

Soit Π l'ensemble des éléments premiers de R (nous ne considérons pas comme distincts deux éléments qui engendrent le même idéal premier, c'est-à-dire sont égaux à un facteur inversible près). L'ensemble E_p des éléments de E dont l'annulateur est une puissance de (p) est un sous-groupe de E que l'on appelle composante primaire de E associée à l'élément premier p .

E est somme directe des sous-groupes E_p et comme de plus tout endomorphisme de E conserve tous les E_p , l'étude d'un groupe de torsion se ramène à celle d'un groupe primaire.

II. — Groupes abéliens primaires.

On dit que E est un groupe abélien primaire associé à l'élément premier p s'il vérifie (1), (2), (3) et si l'annulateur de tout $u \in E$ est une puissance de (p) .

QUELQUES DÉFINITIONS. — Dans ce qui suit E est primaire, associée à p .

On dit que E est du type p^n s'il est monogène et si $N(E) = (p^n)$. Il en résulte $E \cong R/(p^n)$ et les seuls sous-groupes de E sont

$$E \supset pE \supset \dots \supset p^n E = 0.$$

On dit que E est du type p^∞ si $N(E) = 0$ et si tout sous-groupe de E d'annulateur (p^n) est du type p^n . Il faut démontrer l'existence de tels groupes, ce qui sera l'occasion d'étudier leur structure. On a de façon générale

$$E = \bigcup_n E_n \quad \text{où} \quad E_n = \{ u \in E \mid p^n u = 0 \}.$$

Ici E_n doit être du type p^n de sorte que si E existe c'est une limite inductive de groupes du type p^n . Soit $E_1, \dots, E_n$ une suite de groupes tels que E_n est du type p^n . On peut identifier E_{n-1} avec pE_n car ces deux groupes sont isomorphes. Cela permet de définir $E = \bigcup_n E_n$ qui est du type p^∞ , en effet : il est clair que $N(E) = 0$, soit d'autre part F un sous-groupe de E , on a $F = \bigcup_n F \cap E_n$ et comme

$$F \cap E_n = E_{n'} \quad (n' \leq n)$$

il en résulte $F = E_k$ si $N(F) = (p^k)$ et $F = E$ si $N(F) = 0$.

En résumé tout groupe E du type p^∞ est une limite inductive de groupes E_n du type p^n et les seuls sous-groupes de E sont les E_n et E . Deux groupes du type p^∞ sont isomorphes.

On appelle *hauteur* de $u \neq 0$ et $u \in E$ la borne supérieure $h(u)$ des entiers n tels que $p^n v = u$ soit résoluble en v dans E . Il se peut que $h(u) = \infty$; par exemple si E est du type p^∞ on a $h(u) = \infty$ pour tout $u \in E$.

On appelle *racine* de E un élément u qui est contenu dans un sous-groupe de E du type p^∞ . Si u est une racine, on a $h(u) = \infty$, mais la réciproque n'est pas vraie.

Remarque. — Soit E vérifiant seulement (1), (2), (3). On pourra dire que $u \in E$ est une racine associée à p si u est contenu dans un sous-groupe du type p^∞ de E.

On peut aussi définir $h_{pF}(u)$ où $u \in F \subset E$ comme la borne supérieure des entiers n tels que $p^n v = u$ est résoluble en v dans F.

STRUCTURE DES GROUPES ABÉLIENS PRIMAIRES. — Si l'annulateur de E est (p^α) on sait (théorème 7) que E est somme directe de groupes du type p^β ($\beta \leq \alpha$).

La structure d'un groupe primaire E est également connue dans le cas où E a un ensemble dénombrable de générateurs : Prufer [18] a montré que la condition nécessaire et suffisante pour que E soit somme directe de groupes du type p^n ou p^∞ est que tout $u \in E$ soit une racine ou soit de hauteur finie; dans le cas général Ulm [22] a donné un système complet d'invariants de structure pour cette question voir aussi Zippin [23] et Kaplansky-Mackey [26].

La structure d'un groupe abélien primaire quelconque n'est pas connue. Nous allons étudier quelques propriétés d'un tel groupe.

GRUPE DE RACINES. — Soit E vérifiant (1), (2), (3), F_p un sous-groupe de racines associées à $p \in \Pi$ (c'est-à-dire que tout $u \in F_p$ est contenu dans un groupe du type p^∞ contenu dans F_p), $F = \sum_p F_p$,

G un sous-groupe de E disjoint de F. Il existe un sous-groupe F' contenant G et tel que $E = F + F'$.

Cette propriété est une conséquence du théorème suivant :

THÉORÈME 30. — Soit E vérifiant (1), (2), (3), F un sous-groupe de E tel que l'équation $av = u$ soit résoluble en v dans F pour tout $u \in F$, $a \in R$, soit enfin G un sous-groupe de E disjoint de F. Il existe $F' \supset G$ tel que $E = F + F'$.

Donnons une démonstration rapide de ce théorème qui figure dans R. Baer [2]. Soit F' maximal parmi les sous-groupes de E contenant G

et disjoints de F . Nous allons montrer que $E = F + F'$. Supposons qu'il existe $u \notin F + F'$; deux cas sont à distinguer :

Cas 1. — $(u) \cap (F + F') = 0$. Alors $F'' = (u) + F'$ vérifie $F'' \supset G$ et $F'' \cap F = 0$ ce qui contredit la maximalité de F' .

Cas 2. — $(u) \cap (F + F') \neq 0$. Cela signifie que l'annulateur (a) de u modulo $F + F'$ est $\neq 0$. Soit p un diviseur premier de a ; quitte à multiplier u par a/p on peut supposer que $pu \in F$. On a donc $pu = v + v'$, avec $v \in F$, $v' \in F'$; d'après l'hypothèse sur F il existe $w \in F$ tel que $pw = v$. En substituant $u - w$ (qui $\notin F + F'$) à u on peut finalement supposer que $pu \in F'$. On a alors $(u, F') \cap F = 0$. Supposons que $au + u' \in F$ avec $u' \in F'$; comme $F \cap F' = 0$ il faut que $(a, p) = (1)$, c'est-à-dire $\lambda a + \mu p = 1$. On en déduit $(1 - \mu p)u + \lambda u' \in F$ ou $u \in F + F'$, ce qui est une contradiction.

COROLLAIRE. — Soit E un groupe de racines associées à $p \in \Pi$; E est somme directe de groupe du type p^∞ .

THÉORÈME 31. — Soit E un groupe abélien primaire associé à $p \in \Pi$; $P = \{u \in E \mid pu = 0\}$, $P_n = P \cap p^n E$. Une condition nécessaire et suffisante pour que E soit un groupe de racines est que $P_n = P$ pour tout entier n .

La condition est nécessaire puisque pour un groupe de racines $pE = E$. Pour la suffisance nous montrerons que $P_n = P$ ($n = 1, 2, \dots$) entraîne $h(u) = \infty$ pour tout $u \in E$.

Pour $u \in P$ on a $h(u) = \infty$ puisque $p^n E \supset P$ quel que soit n . Pour u quelconque nous opérerons par récurrence sur l'exposant α de l'annulateur (p^α) de u . Soit à résoudre $p^\beta v = u$ en v . On sait résoudre en w l'équation $p^{\beta+1} w = pu$ car $N(pu) = (p^{\alpha-1})$. De $p(u - p^\beta w) = 0$ résulte qu'il existe w' tel que

$$p^\beta w' = u - p^\beta w \quad \text{ou} \quad p^\beta (w + w') = u, \quad \text{d'où} \quad h(u) = \infty.$$

De $h(u) = \infty$, $u \in E$ résulte que tout $u \in E$ est contenu dans un groupe du type p^∞ , c'est-à-dire que E est un groupe de racines.

DÉCOMPOSITION PARTIELLE CANONIQUE D'UN GROUPE ABÉLIEN. — Soit E vérifiant (1), (2), (3), et $p \in \Pi$. Posons $P = \{u \in E \mid pu = 0\}$, $P_n = P \cap p_n E$; P et P_n sont des sous-groupes de E qui sont contenus dans la compo-

sante primaire E_p de E . Les $u \in P$, $\notin P_i$ sont tels que $h_p(u) < i$. L'annulateur de P étant (p) on peut considérer P comme espace vectoriel sur le corps $R/(p)$. Ceci nous montre qu'il existe un sous-groupe ou) sous-espace, c'est la même chose) Q_i tel que $P_{i-1} = P_i + Q_i$. On a alors

$$P = Q_1 + \dots + Q_n + P_n,$$

avec $h_p(u) = i - 1$ si $u \in Q_i$ et $h_p(u) \geq n$ si $u \in P_n$.

Nous allons démontrer le théorème suivant de T. Szele [21].

THÉORÈME 32. — *On peut trouver une décomposition*

$$E = F_1 + \dots + F_n + E_n$$

telle que $F_i \cap P = Q_i$, $p^i F_i = 0$ ($i = 1, \dots, n$) et $E_n \cap P = P_n$ (les hypothèses et les notations sont celles que l'on vient de préciser).

Posons $Q_i = \sum_{j \in I_i} (u_{ij})$; comme $h(u_{ij}) = i - 1$ il existe v_{ij} tel que $p^{i-1} v_{ij} = u_{ij}$ et en se reportant à la démonstration du théorème 7 on voit que la somme $E'_n = \sum_{ij} (v_{ij})$ est bien directe. De la définition des v_{ij} résulte qu'en posant $F_i = \sum_{j \in I_i} (v_{ij})$, on a $F_i \cap P = Q_i$.

Reste à trouver E_n tel que $E = E_n + E'_n$. Désignons par $\bar{H}$ l'image canonique d'une partie H de E dans le groupe quotient $\bar{E} = E/p^n E$. L'annulateur de $\bar{E}$ est (p^n) et en se reportant au théorème 7 on voit qu'on peut trouver une décomposition de E en groupes monogènes, prolongeant la décomposition $\Sigma + (\overline{v_{ij}})$, c'est-à-dire qu'il existe E_n tel que $\bar{E} = \bar{E}_n + \bar{E}'_n$. Nous supposons que $E_n \supset p^n E$, ce qui ne change rien. Nous allons montrer que $E = E_n + E'_n$. D'abord $E = (E_n, E'_n)$, car l'égalité est vraie modulo $p^n E$ et $E_n \supset p^n E$. Ensuite $E_n \cap E'_n = 0$. Soit $u \in E_n \cap E'_n$; comme $E_n \cap E'_n = 0 \pmod{p^n E}$, on a $u \in p^n E$; de $p^n E \cap E'_n = 0$ résulte alors $u = 0$. On a enfin $p^n E_n = p^n E$, donc $E_n \cap P = P_n$, ce qui achève la démonstration.

COROLLAIRE. — *Soit E vérifiant (1), (2), (3) et indécomposable. Ou bien il existe $p \in \Pi$ tel que E est du type p^n ou du type p^∞ . Ou bien E est sans torsion (tout élément de E a pour annulateur zéro).*

LE CENTRE DE L'ANNEAU R' DES ENDOMORPHISMES DE E . — Nous nous proposons de démontrer que si E est un groupe de torsion on a $R'' = \overline{R}$. En fait nous allons établir le résultat un peu plus général suivant :

THÉOREME 33. — *Soit E vérifiant (1), (2), (3). Tout $\theta \in R''$ conserve tous les sous-groupes de torsion de E .*

Il suffit de s'occuper des sous-groupes de E_p = ensemble des $u \in E$ dont l'annulateur est une puissance de $p \in \Pi$. Nous distinguerons deux cas pour le groupe E_p (notations du théorème 32).

1° Il existe α tel que $P_n = P_\alpha$ pour $n \geq \alpha$. Alors E_p est terme direct d'une décomposition de E . Le théorème s'obtient en remarquant que tout endomorphisme de E_p peut se prolonger à E , et en utilisant le lemme suivant dont la démonstration est analogue à celle du théorème 18.

LEMME 1. — *Si E vérifiant (1), (2), (3) est somme directe de groupes monogènes ou du type p^∞ on a $R'' = \overline{R}$.*

2° Il existe une infinité de Q_n non nuls. Soit alors $u \in E_p$ et $N(u) = (p^\alpha)$; il existe $n > \alpha$ tel que $Q_n \neq 0$, ce qui permet d'écrire $E = (v) + E'$ avec $N(v) = (p^n)$. Le théorème résulte du lemme suivant :

LEMME 2. — *Tout sous-groupe (u) homomorphe à un sous-groupe (v) qui est terme direct d'une décomposition de E est conservé par tout $\theta \in R''$.*

Comme (v) est terme direct d'une décomposition de E : $E = E' + (v)$, on a $\theta(v) \subset (v)$. Soit d'autre part $\sigma \in R'$ défini par $\sigma E' = 0$, $\sigma v = u$ [on peut poser $\sigma v = u$ car $(u) \sim (v)$]. Il vient

$$\theta(u) = \theta\sigma(v) = \sigma\theta(v) \subset \sigma E = \sigma(v) = (u).$$

Si E est un groupe de torsion, tout $\theta \in R''$ conserve tous les sous-groupes de E , puisque ce sont des groupes de torsion; on a donc $R'' = R^* = \overline{R}$.

Pour un opérateur linéaire de torsion le résultat qui précède s'écrit $r''(A) = \overline{r(I, A)}$.

III. — Groupes cycliques généralisés.

Soit E un groupe cyclique généralisé, c'est-à-dire vérifiant (1), (2), (3) et la condition : Tout sous-groupe de E qui a un nombre fini de générateurs est cyclique (= monogène).

Il se peut que E soit un groupe de torsion. S'il n'en est pas ainsi il existe $u \in E$ d'annulateur zéro; nous allons montrer que dans ce cas E est nécessairement sans torsion. Soit $v \in E$; on a $(u, v) = (w)$ et $(u) \subset (w)$ entraîne $N(w) = 0$. Comme $v = aw$ avec $a \in R$ et que R n'a pas de diviseurs de zéro l'annulateur de v est aussi zéro. Nous avons donc démontré le résultat suivant :

THÉOREME 34. — *Si E est un groupe cyclique généralisé, E est un groupe de torsion, ou un groupe sans torsion.*

GROUPES CYCLIQUES GÉNÉRALISÉS DE TORSION. — Soit $E = \sum_{p \in \pi} E_p$ la décomposition de E en somme directe de groupes primaires. E_p sera aussi un groupe cyclique généralisé, donc nécessairement du type p^n ou du type p^∞ d'après l'étude faite au paragraphe 3. Inversement il est facile de vérifier qu'une somme directe de groupes E_p du type p^n ou p^∞ (un seul groupe par élément premier) est un groupe cyclique généralisé.

Ceci permet de caractériser très simplement un groupe cyclique généralisé au moyen d'une fonction $v(p)$ définie sur Π et à valeurs dans l'ensemble $0, 1, 2, \dots, \infty$. Pour cela on pose $v(p) = n$ si E_p est du type p^n et $v(p) = \infty$. Il y a correspondance biunivoque entre les fonctions $v(p)$ et les groupes cycliques généralisés de torsion.

Étudions maintenant le treillis $\mathcal{L}$ des sous-groupes d'un groupe cyclique généralisé. Dans ce but commençons par considérer un groupe abélien quelconque de torsion E . $\mathcal{L}$ est isomorphe au produit direct des treillis $\mathcal{L}_p$ des sous-groupes des composantes primaires E_p . Pour que $\mathcal{L}_p$ soit distributif il est en particulier nécessaire que $P = \{u \in E_p \mid pu = 0\}$ soit un espace vectoriel de dimension 1 sur le corps $R/(p)$. On vérifie sans peine que $\dim P = 1$ si et seulement si E_p est du type p^n ou du type p^∞ . Dans ces deux derniers cas $\mathcal{L}_p$ est un

ensemble totalement ordonné, donc est distributif. Pour un groupe de torsion il y a ainsi équivalence entre les propriétés :

- (1) E est un groupe cyclique généralisé;
- (2) Le treillis $\mathcal{L}$ est distributif.

Étudions l'anneau des endomorphismes d'un groupe cyclique généralisé. $\theta \in R'$ conserve les composantes primaires E_p et aussi tous les sous-groupes de E_p car ces derniers sont de la forme $p^{-1}(0) \cap E_p$. Il en résulte que $R' = \bar{R}$.

Inversement $R' = \bar{R}$ entraîne (pour un groupe avec torsion) que E est un groupe cyclique généralisé. En effet si E_p n'est pas du type p^n ou p^∞ c'est un groupe décomposable en $E_p = F + F'$, considérons la projection sur F qui est un endomorphisme $\theta \in R'$. Soit $u \neq 0, \in F$ et tel que $pu = 0$; $u' \neq 0, \in F'$ et tel que $pu' = 0$. On a $\theta(u + u') = \theta u = u$ et, comme $(u + u') \cap (u) = 0$, on a $\theta(u + u') \notin (u + u')$. Cela entraîne $R' \neq \bar{R}$.

Résumons les résultats qui précèdent :

THÉORÈME 35. — *Pour un groupe abélien de torsion les propriétés suivantes sont équivalentes :*

- a. E est un groupe cyclique généralisé;
- b. Les composantes primaires de E sont du type p^n ou p^∞ (ou encore sont indécomposables);
- c. Le treillis des sous-groupes de E est distributif;
- d. $R' = \bar{R}$.

THÉORÈME 35'. — *Pour un opérateur linéaire de torsion les propriétés suivantes sont équivalentes :*

- a. A est non dérogatoire;
- b. Les composantes primaires de A sont du type p^n ou p^∞ (ou encore sont indécomposables);
- c. Le treillis des sous-espaces stables pour A est distributif;
- d. $r'(A) = \overline{r(I, A)}$.

GROUPES CYCLIQUES GÉNÉRALISÉS SANS TORSION. — Dans tout ce qui suit E désigne un groupe généralisé sans torsion. Le quotient de E par un

sous-groupe est encore un groupe cyclique généralisé. En particulier faisons le quotient $E/(u)$. Soit $v \in E$; on a $(u, v) = (w)$, d'où $u = aw$, $v = bw$, d'où $av \in (u)$ ce qui montre que l'annulateur de $\bar{v}$ ($=$ classe de v) est $\neq 0$. $E/(u)$ est donc un groupe cyclique généralisé avec torsion, ce qui va nous permettre de ramener dans une certaine mesure le cas sans torsion au cas avec torsion.

Le groupe $E/(u)$ est caractérisé à une isomorphie près par une fonction $v(p)$ définie plus haut; nous noterons cette fonction $v(u, p)$. Comparons les fonctions $v(u, p)$ et $v(v, p)$. Nous supposons $(u) \supset (v)$, le cas général se ramenant à ce cas en introduisant la fonction intermédiaire $v(w, p)$, où $(w) = (u) \cap (v)$. On a

$$v = au = p_1^{\alpha_1} \dots p_s^{\alpha_s} u, \quad (p_1, \dots, p_s \in \Pi).$$

Posons $E/(u) = \sum_{p \in \Pi} F_p$ et soit $\bar{w} \in F_p$, d'annulateur (p^α) ; cela entraîne que $p^\alpha w \in (u)$, soit $p^\alpha w = bu$; on doit avoir $(p, b) = (1)$ car dans le cas contraire $p^{\alpha-1} w \in (u)$; il existe $\lambda, \mu \in R$ tels que $\lambda p^\alpha + \mu b = 1$, d'où $p^\alpha (\mu w + \lambda u) = u$, ce qui montre que l'on pouvait supposer $p^\alpha w = u$. On en déduit aussitôt :

$$\begin{aligned} v(v, p) &= v(u, p) & \text{si } p &\neq p_1, \dots, p_s; \\ v(v, p_i) &= v(u, p_i) + \alpha_i & (i = 1, \dots, s). \end{aligned}$$

On en déduit que si u et v sont quelconques on a la condition

$$(\Gamma) \quad \sum_{p \in \Pi} |v(u, p) - v(v, p)| < \infty$$

(on convient que $\infty - \infty = 0$).

La condition (Γ) est une relation d'équivalence dans l'ensemble des fonctions $v(p)$; nous désignerons par $\bar{v}$ la classe de v . Si u parcourt E , $v(u, p)$ parcourt une classe $\bar{v}$ ce qui permet de faire correspondre à tout groupe E une classe $\bar{v}$. Nous allons montrer qu'inversement toute classe $\bar{v}$ est associée à un groupe E défini de façon unique à une isomorphie près. Pour cela nous allons utiliser une construction généralisant la notion de somme directe de groupes.

Soit F_i , $i \in I$ une famille de groupes abéliens ayant un même anneau R d'opérateurs; on suppose de plus que F_i contient un groupe G_i

isomorphe à un groupe donné H , et l'on identifie G_i à H au moyen d'un isomorphisme bien déterminé.

Posons $F = \sum_i F_i$, $G = \sum_i G_i$; si $u \in (u_i)$ est un élément de G la correspondance $\theta u = \sum_i u_i$ est un homomorphisme de G sur H ; nous poserons $G' = \bar{\theta}^{-1}(0) = \left\{ u \mid \sum_i u_i = 0 \right\}$. Nous allons étudier le groupe quotient $E = F/G_i$.

E contient quel que soit i un sous-groupe isomorphe à F_i , à savoir l'image canonique $\bar{F}_i$ de F_i ($\bar{F}_i \cong F_i$ résulte de ce que $F_i \cap G' = G_i \cap G' = 0$). On a $\bar{F}_i \cap \bar{F}_j = \bar{G}_i = \bar{G}_j$ ($i, j \in I$), ce qui montre que l'intersection des groupes $\bar{F}_i$ est un groupe isomorphe à H , et que nous identifierons à H ; de plus $E/H \cong \sum_i F_i/H$.

Le groupe E que nous venons de construire généralise bien la notion de somme directe que l'on retrouve en prenant $H = \{0\}$.

Reprenons une classe $\bar{\nu}$ dont ν est un représentant et à tout $p \in \Pi$ associons le groupe E_p défini comme suit : E_p contient un sous-groupe (u_p) d'annulateur 0 ; si $\nu(p) = n$ est fini, $E_p = (u_p^n)$ et $u_p = p^n u_p^n$; si $\nu(p) = \infty$, $E_p = \bigcup_n E_p^n$ où l'on pose $E_p^n = (u_p^n)$, $pu_p^1 = u_p$, $pu_p^2 = u_p^1 \dots$.

On peut identifier les sous-groupes (u_p) en posant $u_p = u$, où u est un générateur d'un groupe $F = (u) \cong R$.

Définissons à partir des E_p un groupe E comme plus haut. Il est facile de vérifier que E est un groupe cyclique généralisé sans torsion auquel est associée la classe $\bar{\nu}$. u et les u_p^i [$p \in \Pi$, $i = 1, \dots, \nu(p)$] forment ce que nous appellerons un système de générateurs canoniques de E . Il nous reste à montrer l'unicité de E . Soit E' tel que $\nu(u', p) = \nu(p)$; en se reportant à l'étude des fonctions $\nu(u, p)$ faite plus haut on voit qu'il existe pour tout p , u_p^i [$i = 1, \dots, \nu(p)$] tels que $pu_p^1 = u'$, $pu_p^2 = u_p^1, \dots$. On vérifie que u' et les u_p^i forment un système de générateurs de E' ce qui permet d'établir un isomorphisme entre E et E' . Tout est démontré.

Nous allons maintenant étudier le treillis des sous-groupes d'un

groupe cyclique généralisé. Nous démontrerons le théorème suivant dû à O. Ore [15]⁽³⁾.

THÉOREME 36. — *Soit E un groupe abélien vérifiant (1), (2), (3), les propriétés suivantes sont équivalentes :*

- a. E est un groupe cyclique généralisé;
- b. le treillis $\mathcal{L}$ des sous-groupes de E est distributif.

« non a » $\rightarrow$ « non b ». — Soit u, v tels que l'on n'ait pas $(u, v) = (w)$. Comme nous avons déjà démontré le théorème pour un groupe de torsion on peut supposer que l'annulateur de u par exemple est nul. (u, v) étant somme directe de groupes monogènes nous pouvons encore supposer que $(u) \cap (v) = 0$. Nous avons alors

$$\begin{aligned} ((u) \cap (v), (u + v)) &= (u + v), \\ ((u), (u + v)) \cap ((v), (u + v)) &= (u, v), \end{aligned}$$

ce qui montre que la condition de distributivité pour $\mathcal{L}$ n'est pas toujours remplie.

$a \rightarrow b$. — Il nous reste à faire la démonstration pour E sans torsion. Soit $F, G, H \in \mathcal{L}$. On a $F \cap G \cap H \neq 0$ et il suffit de vérifier la condition de distributivité modulo $F \cap G \cap H$. Cette condition est vérifiée car $E/F \cap G \cap H$ est un groupe cyclique généralisé de torsion.

Étudions maintenant l'anneau des endomorphismes d'un groupe cyclique généralisé sans torsion E. Soit $\bar{v}$ la classe de fonctions associées à E et $v \in \bar{v}$.

THÉOREME 37. — *Une condition nécessaire et suffisante pour que la multiplication par $p \in \Pi$ soit un endomorphisme inversible est que $v(p) = \infty$. On a en outre*

$$R' = r(R, \{p^{-1} \mid v(p) = \infty\}).$$

Si p est un endomorphisme inversible, $p^{-n}u$ existe pour tout $u \in E$, donc $v(p) = \infty$. Inversement si $v(p) = \infty$, on a $v(u, p) = \infty$ pour tout

⁽³⁾ O. Ore considère des groupes quelconques, mais sans opérateurs.

$u \in E$, c'est-à-dire qu'il existe $v \in E$ (nécessairement unique) tel que $pv = u$: p est inversible.

Pour la deuxième partie du théorème nous utiliserons le lemme : Soit $\theta, \sigma \in R'$; s'il existe $u \in E$ tel que $\theta u = \sigma u$, on a $\theta = \sigma$. Soit en effet $v \in E$; on a $bv = au$, d'où $\theta bv = \sigma bv$, d'où $\theta = \sigma$.

Soit $\theta \in R'$; de $p\theta = \theta p$ ($p \in \Pi$) résulte $v(u, p) \leq v(\theta u, p)$. On en déduit

$$\theta u = ap_1^{\alpha_1} \dots p_s^{-\alpha_s} u, \quad \text{où } u \in R, \quad v(p_1) = \dots = v(p_s) = \infty,$$

c'est-à-dire

$$\theta \in r(R, \{p^{-1} \mid v(p_1) = \infty\}).$$

Pour A le théorème 37 signifie que tout commutant de A est une fraction rationnelle en A.

CHAPITRE V.

ANNEAUX COMMUTATIFS ENGENDRÉS PAR DES PROJECTEURS.

Soit E un espace vectoriel sur un corps commutatif K et φ un treillis de projecteurs sur E ; φ est défini par les conditions :

- (1) $P, Q \in \varphi$ entraîne $PQ = QP$, $PQ \in \varphi$, $P \perp Q = P + Q - PQ \in \varphi$
- (2) $P, Q \in \varphi$ et $P \leq Q$ entraîne $Q - P \in \varphi$.

Si $\{P, Q, \dots\}$ est un système commutatif de projecteurs, on désignera par $l(P, Q, \dots)$ le treillis engendré par $P, Q, \dots$.

THÉORÈME 38. — *Tout treillis $\varphi = l(P_1, \dots, P_k)$ engendré par un système commutatif fini de projecteurs peut être mis sous la forme $\varphi = l(Q_1, \dots, Q_s)$, avec $Q_i Q_j = 0$ si $i \neq j$.*

Si l'on ferme l'ensemble $\{P_1, \dots, P_k\}$ pour les opérations $\perp$ et produit on obtient encore un système fini car un projecteur est idempotent ; on peut donc supposer que $\{P_1, \dots, P_k\}$ vérifie (1). Soit Q_1 un projecteur minimal de l'ensemble $\{P_1, \dots, P_k\}$; on a alors $Q_1 P_i = Q_1$ ou zéro selon que $Q_1 \leq P_i$ est réalisé ou non. On peut écrire pour $i = 1, \dots, k$, $P_i = Q_1 P_i + Q_i$ avec $Q_i Q_1 = 0$. Les Q_i

forment un système de moins de k projecteurs et vérifiant (I), ce qui démontre le théorème par récurrence.

Définition. — Nous dirons qu'un treillis φ est complet si quel que soit $\psi \subset \varphi$ les projecteurs $\prod_{P \in \psi} P$ et $\sum_{P \in \psi} \dot{+} P$ ont un sens et appartiennent à φ .

Précisons le sens de cette définition. Nous poserons $\bigcap_{P \in \psi} PE = E_\psi$ et $\bigcup_{P \in I(\psi)} (I - P)E = E'_\psi$. On vérifie que $E_\psi \cap E'_\psi = 0$, mais on n'a pas nécessairement $E = E_\psi + E'_\psi$. Si cette dernière condition est réalisée la projection sur E_ψ parallèlement à E'_ψ a un sens et on l'appelle $\prod_{P \in \psi} P$.

Posons ψ étant toujours une partie de φ : $\psi^* = \{P \mid I - P \in \psi\}$; lorsque P parcourt ψ , $I - P$ parcourt un treillis φ^* . On a encore $E_{\psi^*} \cap E'_\psi = 0$; si de plus $E_{\psi^*} + E'_\psi = E$ la projection sur E_{ψ^*} parallèlement à E'_ψ a un sens et on l'appelle $\sum_{P \in \psi} \dot{+} P$. On a les relations

$$\prod_{P \in \psi} P = I - \sum_{P \in \psi^*} \dot{+} P, \quad \sum_{P \in \psi} \dot{+} P = I - \prod_{P \in \psi^*} P.$$

ÉTUDE DE L'ANNEAU ENGENDRÉ PAR UN TREILLIS COMPLET φ DE PROJECTEURS.
— Soit $R = r(\varphi)$ l'anneau engendré par φ . Nous munirons l'ensemble $\mathcal{O}$ des opérateurs linéaires sur E de la topologie finie introduite au chapitre précédent. La fermeture de R sera toujours notée $\bar{R}$. L'ensemble des projecteurs de R sera noté R^p ; on a ici $R^p = \varphi$. Dans la suite P et Q désigneront toujours des projecteurs de φ .

THÉORÈME 39. — $(\bar{R})^p = R^p$.

Soit $P \in (\bar{R})^p$ et $u \in PE$, $v \in (I - P)E$. Il existe $Q_{uv} \in R^p$ tel que $Q_{uv}u = Pu = u$ et $Q_{uv}v = Pv = 0$ (il existe, d'après la définition de $\bar{R}$, $A \in R$ vérifiant $Au = Pu$ et $Av = 0$; d'après le théorème 38 on peut écrire $A = \sum \lambda_i P_i$ ou $P_i \in \varphi$ et $P_i P_j = 0$ si $i \neq j$; on peut supprimer de

la somme les P_i tels que $P_i u = 0$; $Au = u$ entraîne alors $\lambda_i = 1$ et A est un projecteur). On a

$$P = \prod_{v \in (I-P)E} \left(\sum_{u \in PE} \vdash Q_{uv} \right) \in R$$

car R^p est complet.

THÉOREME 40. — Si E_R est monogène, c'est-à-dire si $E = Ru$, tout sous-espace de E stable pour R est de la forme $F = PE$ avec $P \in R^p$.

Soit $v \in F$ stable pour R . D'après l'hypothèse $E = Ru$ il existe des $a_i \in K$ et $P_i \in \varphi$ tels que $v = \left(\sum_{i=1}^k a_i P_i \right) u$; d'après le théorème 38 on peut supposer que $P_i P_j = 0$ si $i \neq j$. On a $P_i v = a_i P_i u \in F$, ce qui montre que $F = \{ a P u \mid a \in K, P \in \varphi, P u \in F \}$, d'où $F \subset PE$ où $P = \sum_{Q u \in F} \vdash Q$. Il y a égalité : $F = PE$ car si $Q u \in F$ on a $Q E \subset F$.

COROLLAIRE. — Comme E est stable pour R , $E = Ru$ implique $I \in \varphi = R^p$.

Si F est un sous-espace de E stable pour R nous désignerons par φ_F le treillis des sous-espaces de la forme PF et par $\mathcal{L}_F$ le treillis des sous-espaces stables pour R et contenus dans F . On a $\mathcal{L}_F \supset \varphi_F$. Il est d'autre part naturel d'établir entre φ et φ_F la correspondance $P \rightarrow PF$; φ_F s'obtient en faisant le quotient de φ par la relation d'équivalence « $P \sim Q$ si et seulement si $PF = QF$ ». φ_F est homomorphe à φ , ce que nous écrirons $\varphi_F \sim \varphi$; si il y a isomorphisme nous écrirons $\varphi_F \cong \varphi$.

THÉOREME 41. — Quelque soit $F \in \mathcal{L}_E$ il existe $G \in \mathcal{L}_E$ tel que $E = F + G$.

Soit G maximal parmi les éléments de $\mathcal{L}_E$ qui vérifient $G \cap F = 0$. Nous pouvons pour la démonstration supposer que $I \in R$ car $\mathcal{L}_E$ est le même pour R et $r(R, I)$ et d'autre part si φ est complet, $l(\varphi, I)$ l'est aussi. Supposons qu'il existe $u \notin F \vdash G$; d'après le théorème 40 on peut écrire

$$Ru \cap (F + G) = P(Ru) \vdash R(Pu);$$

comme $Ru = PRu + (I - P)Ru$, on a

$$(I - P)Ru \cap (F + G) = 0.$$

Le sous-espace $G' = (I - P)Ru + G$ vérifie $G' \cap F = 0$, ce qui contredit la maximalité de G ; on avait donc $F + G = E$.

THÉORÈME 42. — *Si $I \in \varphi$ il existe $F \in \mathcal{L}_E$ tel que $\mathcal{L}_F = \varphi_F \cong \varphi$.*

Soit Φ la famille des $F \in \mathcal{L}_E$ qui vérifient $\mathcal{L}_F = \varphi_F$. Il existe des $F \in \Phi$ et $\neq 0$; d'après le théorème 40 il en est ainsi de tous les sous-espaces F de la forme Ru . Nous allons montrer que Φ est inductive; le théorème résultera de cette propriété, en effet : Soit F un élément maximal de Φ ; F est $\neq 0$ comme on l'a remarqué plus haut; si l'on n'avait pas $\varphi_F \cong \varphi$ cela entraînerait qu'il existe P et Q tels que $P \neq Q$ et $PF = QF$. Quitte à remplacer P par PQ et Q par $P + Q - PQ$ on peut supposer que $P < Q$. On a alors $(Q - P)F = 0$ et en prenant $u \in (Q - P)E$ on vérifie que $Ru \cap F = 0$ puis que $F' = F + Ru \in \Phi$ ce qui contredit la maximalité de F . On avait donc $\varphi_F \cong \varphi$.

Pour démontrer que Φ est inductive considérons une sous-famille $\{F_\alpha \mid \alpha \in J\} \subset \Phi$ totalement ordonnée (par la relation d'inclusion).

Nous poserons $F = \bigcup_{\alpha} F_{\alpha}$; soit $G \in \mathcal{L}_F$ on a $G = \bigcup_{\alpha} G \cap F_{\alpha}$. De la définition de Φ résulte qu'on peut écrire

$$F_{\alpha} \cap G = P_{\alpha} F_{\alpha} \quad (P_{\alpha} \in \varphi);$$

$$F_{\alpha} = P_{\alpha\beta} F_{\beta}, \quad \text{avec} \quad P_{\alpha\beta} \in \varphi \quad \text{si} \quad \alpha < \beta \quad (\alpha < \beta \text{ signifie } F_{\alpha} \subset F_{\beta}).$$

On a $F_{\alpha} = \left(\prod_{\beta > \alpha} P_{\alpha\beta} \right) F$, en effet

$$\left(\prod_{\beta > \alpha} P_{\alpha\beta} \right) F = \bigcap_{\beta > \alpha} P_{\alpha\beta} F \supset \bigcap_{\beta > \alpha} P_{\alpha\beta} F_{\beta} = F_{\alpha}$$

et d'autre part si $u \in \bigcap_{\beta > \alpha} P_{\alpha\beta} F$ on a $u \in F$, donc $u \in F_{\gamma}$ pour un certain indice γ , donc

$$u \in \left(\prod_{\beta > \alpha} P_{\alpha\beta} \right) F_{\gamma} \subset F_{\alpha}.$$

On a

$$G = \bigcup_{\alpha} F_{\alpha} \cap G = \bigcup_{\alpha} P_{\alpha} F_{\alpha} = \bigcup_{\alpha} \left[P_{\alpha} \left(\prod_{\beta > \alpha} P_{\alpha\beta} \right) F \right].$$

Posons $\prod_{\beta > \alpha} P_{\alpha\beta} = Q_{\alpha}$; il vient $F_{\alpha} = Q_{\alpha}F$ et en posant $Q'_{\alpha} = \prod_{\beta > \alpha} Q_{\beta}$, on a encore $F_{\alpha} = Q'_{\alpha}F$ avec $Q'_{\alpha} > Q'_{\beta}$ si $\alpha > \beta$. Dans $F_{\alpha} \cap G = P_{\alpha}F_{\alpha}$ on peut remplacer P_{α} par $P'_{\alpha} = \prod_{\beta > \alpha} P_{\beta}$ car

$$P'_{\alpha}F_{\alpha} = \bigcap_{\beta > \alpha} P_{\beta}F_{\alpha} = P_{\alpha}F_{\alpha} = F_{\alpha} \cap G;$$

on a aussi $P'_{\alpha} > P'_{\beta}$ si $\alpha > \beta$. On en déduit :

$$G = \bigcup_{\alpha} (P'_{\alpha}Q'_{\alpha}F) = \left(\sum_{\alpha} P'_{\alpha}Q'_{\alpha} \right) F \in \varphi_F,$$

donc $\varphi_F \cong \varphi$ et le théorème est démontré.

THÉORÈME 43. — *Si $I \in \varphi$ il existe une famille de sous-espaces $F_i \in \mathcal{L}_E$ tels que $\mathcal{L}_{F_1} \cong \varphi$, $\mathcal{L}_{F_i} = \varphi_{F_i}$, $\varphi_{F_i} \sim \varphi_{F_j}$ si $i > j$ (i, j parcourent l'ensemble des ordinaux), $E = \sum_i F_i$.*

L'existence de F_1 résulte du théorème 42. Le théorème 41 montre qu'il existe $E_1 \in \mathcal{L}_E$ tel que $E = E_1 + F_1$. Dans E_1 , φ induit un treillis $\varphi_1 \sim \varphi$ (φ_1 est le quotient de φ par la relation d'équivalence $P \sim Q$ si et seulement si $PE_1 = QE_1$). On peut trouver dans E_1 , F_2 tel que $\mathcal{L}_{F_1} = \varphi_{F_2}$, ..., ce qui démontre le théorème [pour un ordinal i n'ayant pas de précédent on définira E_i par $E_i \in \mathcal{L}_E$ et $\left(\sum_{j > i} F_j \right) + E_i = E$].

ÉTUDE DES ANNEAUX R' ET R'' . — Nous supposons toujours que R est engendré par un treillis complet φ de projecteurs. Rappelons que $R \subset R \subset R'' \subset R'$.

THÉORÈME 44. — On a $R'' = p(\bar{R}, I)$.

Il est équivalent de démontrer que si $I \in R$ on a $R'' = R$; nous supposons donc que $I \in R$. Soit $E = \sum_i E_i$ une décomposition de E

qui vérifie les conditions du théorème 43. Nous appellerons I_i la projection sur F_i . On a $I_i \in R'$ ce qui entraîne la décomposition en somme sous-directe

$$R'' \subset \sum_i + (I_i R)'' = \sum_i + (R_i)'';$$

on a posé $R_i = I_i R =$ anneau induit dans $I_i E$. Ceci nous conduit à étudier le cas où $\mathcal{L}_E = \varphi_E$.

Supposons maintenant $\mathcal{L}_E = \varphi_E$ et soit $u \in E$. On a $Ru = PE$ puisque $Ru \in \mathcal{L}_E = \varphi_E$. Soit $B \in R'$, la condition $Bp.P$ entraîne $Bu \in Ru$, c'est-à-dire l'existence de $A \in R$ tel que $Bu = Au$. L'égalité $B = A$ étant valable en u sera valable dans tout Ru . Nous allons montrer que $B \in \bar{R}$. Soit $u_1, \dots, u_n \in E$; il faut trouver $A \in R$ tel que $Bu_i = Au_i (i = 1, \dots, n)$. On peut trouver $A_1 \in R$ tel que $Bu_1 = A_1 u_1$. Soit $R(u_1, \dots, u_n) = PE$ et $Ru_1 = P_1 E$; de $Bu_1 = A_1 u_1$ résulte $B = A_1$ dans Ru_1 . On a $E = P_1 E + (I - P_1)E$; on peut trouver A_2 tel que $B(I - P_1)u_2 = A_2 u_2$, d'où $B = A_2$ dans $(I - P_1)Ru_2$, etc. D'où finalement

$$B = P_1 A_1 + \dots + P_n A_n \quad \text{dans} \quad R(u_1, \dots, u_n).$$

Ainsi $\mathcal{L}_E = \varphi_E$ entraîne $R' = R$, donc $R'' = R = R'$.

Revenons au cas général $\mathcal{L}_E \neq \varphi_E$; ce qui précède montre que $R'' \subset \sum_i + \bar{R}_i$. Soit $B \in R''$ et $A_i \in \bar{R}$ vérifiant $Bu = A_i u$ si $u \in F_i$. Nous allons montrer que $A_i = A_1$, ce qui entraînera $B = A_1$ et achèvera la démonstration du théorème. Pour cela examinons comment on peut construire $A' \in R'$: Soit $u \in E$ et $P \in \varphi$ tel que $Pu = u$; $A'p.P$ montre qu'il est nécessaire que $A'u \in PE$; il sera donc nécessaire que $A'u \in QE = \left(\prod_{Pu=u} P \right) E$. On peut fixer arbitrairement $A'u$ dans QE car si $v \in QE$, Rv considéré comme groupe à opérateurs sur R est homomorphe à Ru . La condition $A'u = v$ détermine A' dans Ru et il reste à prolonger A' à E tout entier. C'est possible car d'une façon générale si l'on a défini A' dans un sous-espace stable F où il vérifie $A'p.R$, il existe $G \in \mathcal{L}_E$ tel que $F + G = E$, et l'on pourra prolonger A' à $F + Ru$ où u est arbitraire dans G (car alors $Ru \subset G$).

Soit i le premier ordinal tel que $B \neq A_i$ dans F_i . Il se peut que B

coïncide avec A_1 dans un sous-espace de F_i , sous-espace qui est de la forme PF_i ; quitte à se placer dans $(I - P)E$ on pourra supposer que $Bu \neq A_1u$ pour tout $u \in F_i$. Nous allons montrer que c'est impossible.

Soit $Q = \sum_{PF_i=0} \dot{+} P$ et $u \in (I - Q)E_i$; soit $S = \prod_{Pu=u} P$ et $v \neq 0$ appartenant à SF_i . Il existe $A' \in R'$ vérifiant $A'u = v$ d'après ce qu'on a vu plus haut. On a

$$Bv = BA'u = A'Bu = A'A_1u = A_1A'u = A_1v,$$

ce qui est une contradiction, le théorème est démontré.

De la démonstration résulte encore :

THÉORÈME 45. — *Une condition nécessaire et suffisante pour que $R' = p(\bar{R}, I)$ est que $\mathcal{E}_E \cong l(\varphi, I)$.*

SPECTRE DE L'ANNEAU R . — Il est naturel d'appeler l'ensemble φ des projecteurs de $r(R, I)$ le « spectre » de R . Nous avons supposé que φ était un treillis complet, c'est-à-dire inductif pour la relation $P > Q$.

Soit $\bar{\varphi}$ l'ensemble des projecteurs $\neq 0$ de φ et φ_0 le treillis engendré par les projecteurs minimaux de φ . On pourrait appeler φ_0 le spectre ponctuel de R . Posons

$$P_0 = \sum_{P \in \varphi_0} \dot{+} P, \quad \varphi_1 = (I - P_0)\varphi, \quad \varphi_i = \varphi_1 \cap \varphi.$$

Dans $\bar{\varphi}_1$ il n'y a pas de projecteurs minimaux, de sorte que l'on pourrait appeler φ_1 le spectre continu de R . Si $\varphi = \varphi_0$ toute la théorie que nous avons faite est presque triviale. Il est donc intéressant de donner un exemple de spectre continu.

Soit F l'espace vectoriel des fonctions à valeurs réelles définies sur un ensemble infini X et E le quotient de F par la relation d'équivalence « $f \sim g$ si $f(x) = g(x)$ sauf peut-être sur un ensemble fini ». A tout ensemble $S \subset X$ on peut faire correspondre le projecteur P_S défini par $(P_S f)(x) = f(x)$ si $x \in S$ et zéro si $x \notin S$. On a

$$P_S \dot{+} P_{S'} = P_{S \cup S'}, \quad P_S P_{S'} = P_{S \cap S'},$$

de sorte que l'ensemble φ de tous les projecteurs P_S est un treillis véri-

fiant les conditions (1) et (2) et tel que φ ne contient pas de projecteurs minimaux (il n'y a pas d'élément minimal dans l'ensemble des parties infinies de X !).

BIBLIOGRAPHIE.

- [1] R. BAER, *Primary abelian groups and their automorphisms* (*Amer. J.*, t. 59, 1937, p. 99-117).
- [2] R. BAER, *Abelian groups that are direct summands of every containing abelian group* (*Bull. Amer. Math. Soc.*, t. 46, 1940, p. 800-806).
- [3] A. CHÂTELET, *Les groupes abéliens finis et les modules de points entiers*, Paris, 1925.
- [4] MC DUFFEE, *The theory of matrices* (*Ergebnisse der Math.*, 1933).
- [5] P. DUBREIL, *Algèbre*, t. 1, Paris, 1946.
- [6] G. FROBENIUS, *Über vertauschbare Matrizen* (*Sitz. Berl. Akad.*, 1896, p. 601-614).
- [7] H. L. HAMBURGER, *A theorem on commutative matrices* (*J. London Math. Soc.*, t. 24, 1949, p. 200-206).
- [8] N. JACOBSON, *Schur's theorems on commutative matrices* (*Bull. Amer. Math. Soc.*, t. 50, 1944, p. 431-446).
- [9] C. JORDAN, *Groupes abéliens généraux contenus dans les groupes linéaires à moins de sept variables* [*J. Math. pures et appliquées*, (6), t. 3, 1905, p. 213-266].
- [10] G. JULIA, *Introduction mathématique aux théories quantiques*, Paris, 1936.
- [11] M. F. KRAVČŮK, *Über vertauschbaren Matrizen* (*Rend. Circ. Mat. Palermo*, t. 51, 1927, p. 126-130).
- [12] W. KRULL, *Über verallgemeinerte endliche Abelsche Gruppen* (*Math. Z.*, t. 23, 1925, p. 161-196).
- [13] W. KRULL, *Theorie und Anwendung der verallgemeinerten Abelschen Gruppen* (*Sitz. Heidel.*, t. 1, 1926, p. 1-32).
- [14] A. KUROSH, *Primitive Torsionsfrei Abelsche Gruppen vom endlichen Range* (*Ann. Math.*, t. 37, 1936, p. 175-203).
- [15] O. ORE, *Structures and group theory*, II (*Duke J.*, t. 4, 1938, p. 247-269).

- [16] H. B. PHILIPPS, *Functions of matrices* (*Amer. J.*, t. 41, 1919, p. 266-278).
- [17] H. PRUFER, *Theorie der Abelschen Gruppen* (*Math. Z.*, t. 20, 1924, p. 165-187).
- [18] H. PRUFER, *Untersuchungen über die Zerlegbarkeit der abzählbaren primären Abelschen Gruppen* (*Math. Z.*, t. 17, 1923, p. 35-61).
- [19] K. SHODA, *Über die mit einer Matrix vertauschbaren Matrizen* (*Math. Z.*, t. 29, 1929, p. 696-712).
- [20] J. SCHUR, *Zur Theorie der vertauschbaren Matrizen* (*Crelle J.*, t. 130, 1905, p. 66-76).
- [21] T. SZELE, *Sur la décomposition directe des groupes abéliens* (*C. R. Acad. Sc.*, t. 229, 1939, p. 1052-1053).
- [22] H. ULM, *Zur Theorie der abzählbar-unendlichen Abelschen Gruppen* (*Math. Ann.*, t. 107, 1933, p. 774-803).
- [23] L. ZIPPIN, *Countable torsion groups* (*Ann. Math.*, t. 36, 1935, p. 86-99).
- [24] B. L. VAN DER WAERDEN, *Modern Algebra*, Berlin, 1930.
- [25] J. H. M. WEDDERBURN, *Note on Algebra* (*Amer. J.*, t. 38, 1937, p. 854-856).
- [26] I. KAPLANSKY et G. W. MACKEY, *A generalisation of Ulm's theorem* (*Summa Bras. Math.*, t. 13, 1951, p. 1-8).



TABLE DES MATIÈRES.

INTRODUCTION.

CHAPITRE I.

Opérateurs linéaires sur un espace vectoriel à n dimensions.

1. Espaces vectoriels. Opérateurs linéaires.....	5
2. Étude d'un opérateur linéaire.....	6
3. Treillis des sous-espaces stables pour un opérateur linéaire.....	11

CHAPITRE II.

Anneaux particuliers d'opérateurs linéaires sur un espace à n dimensions. Permutabilité.

1. Généralités.....	13
2. Treillis de projecteurs.....	15
3. Étude des anneaux $r(\Lambda)$, $r(I, \Lambda)$, $r'(\Lambda)$, $r''(\Lambda)$	16
4. Permutabilité.....	19
5. Anneaux commutatifs complètement réductibles.....	22

CHAPITRE III.

Anneaux commutatifs d'opérateurs sur un espace vectoriel à n dimensions.

1. Anneaux commutatifs d'opérateurs linéaires.....	23
2. Anneaux commutatifs primaires.....	24
3. Anneaux commutatifs nilpotents.....	28
4. Relations avec les systèmes hypercomplexes commutatifs. Applications..	36

CHAPITRE IV.

Opérateurs linéaires sur un espace vectoriel quelconque.

1. Considérations générales.....	44
2. Groupes abéliens primaires.....	47
3. Groupes cycliques généralisés.....	52

CHAPITRE V.

Anneaux commutatifs engendrés par des projecteurs.

DEUXIÈME THÈSE



PROPOSITIONS DONNÉES PAR LA FACULTÉ.

Espaces vectoriels topologiques



Vu et approuvé :

Paris, le 11 juin 1953.

LE DOYEN DE LA FACULTÉ DES SCIENCES,

A. CHÂTELET.

Vu et permis d'imprimer :

LE RECTEUR DE L'ACADÉMIE DE PARIS,

J. SARRAILH.



PARIS. — IMPRIMERIE GAUTHIER-VILLARS,

Quai des Grands-Augustins, 55.

144808-54

Dépôt légal, Imprimeur, 1954, n° 976

PARIS. — IMPRIMERIE GAUTHIER-VILLARS
144808 Quai des Grands-Augustins, 55.
